UNIVERSIDAD TÉCNICA AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL.

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS.

Tema:

Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo

---

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de investigación, presentado previo a la obtención del título de Ingeniero en Sistema Computacionales e Informáticos.

LÍNEA DE INVESTIGACIÓN: Administración de Recursos

AUTOR: Oscar Marcelo Silva Miranda

TUTOR: Ing. Edison Álvarez

AMBATO – ECUADOR
JULIO 2019

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación sobre el tema "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA OCTAVE DE LOS PROCESOS DE RECAUDACIONES Y PERMISOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO (GAD) DE SAN PEDRO DE PELILEO." del señor Oscar Marcelo Silva Miranda, estudiante de la Carrera de Ingeniería Sistema Computacionales e Informáticos, de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad con el numeral 7.2 de los lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, julio del 2019

EL TUTOR

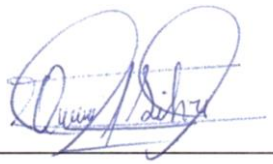
Ing. Edison Homero Álvarez Mayorga Mg.

.

AUTORÍA

El presente Proyecto de Investigación titulado: "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA OCTAVE DE LOS PROCESOS DE RECAUDACIONES Y PERMISOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO (GAD) DE SAN PEDRO DE PELILEO", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato julio, 2019



Oscar Marcelo Silva Miranda

CC. 1804583100

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato julio, 2019

Oscar Marcelo Silva Miranda

CC. 1804583100

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes, Ing. Carlos Núñez e Ing. PhD. Víctor Guachimbosa revisó y aprobó el Informe Final del Proyecto de Investigación titulado "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA OCTAVE DE LOS PROCESOS DE RECAUDACIONES Y PERMISOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO (GAD) DE SAN PEDRO DE PELILEO", presentado por el señor Oscar Marcelo Silva Miranda de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Mg. Elsa Pilar Urrutia Urrutia
PRESIDENTA DEL TRIBUNAL

Ing. Mg. Carlos Núñez
DOCENTE CALIFICADOR

Ing. PhD. Víctor Guachimbosa
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo de grado va dedicado a Dios, que siempre estuvo presente en el caminar de mi vida, bendiciéndome y dándome fortaleza para continuar con mis metas trazadas sin desfallecer.

A mis padres que día a día me apoyaron incondicionalmente brindándome amor, compresión y confianza que permitieron lograr la culminación de mi carrera profesional.

Oscar Marcelo Silva Miranda

AGRADECIMIENTO

El presente trabajo agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas.

A mis padres por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Agradezco a mi tutor de tesis Mg. Edison Álvarez quien con su experiencia, conocimiento y motivación me oriento en la realización de este proyecto

Agradezco a los todos docentes que, con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional en la Universidad Técnica de Ambato.

Al GAD Municipal de San Pedro de Pelileo quienes me abrieron las puertas para realizar el proyecto brindándome su amistad y apoyo, en especial al Ing. Luis Carrasco.

Oscar Marcelo Silva Miranda

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

En el presente trabajo se realizó una Auditoría Informática de los procesos de permiso y recaudación del Gobierno Autónomo Descentralizado de San Pedro de Pelileo, Provincia de Tungurahua, con el objetivo de identificar falencias y establecer controles necesarios que garanticen la seguridad e integridad de la información.

Para el desarrollo de la presente investigación, se utilizó la metodología OCTAVE de Auditoria Informática que cuenta con tres fases, dividida en 8 procesos en los cuales primero se estableció los criterios de medición de riesgo de acuerdo a lo que la entidad requirió, posteriormente se realizó la identificación de activos de información que interactúan con los procesos a auditar, para ello se creó perfiles para cada activo de información y se identificaron los contenedores de estos. Luego se determinaron las distintas áreas de preocupación que son básicamente los problemas que se podrían presentar en la entidad con relación al manejo de las tecnologías de información, con esto se procedió a detallar los escenarios de amenazas potenciales y se creó un árbol de amenazas para cada activo, después se procedió a establecer las consecuencias que podrían ocurrir en el caso de que una amenaza se cumpla, después se midió cualitativamente el grado en el que la institución se vería afectada por cada amenaza y de acuerdo al valor y grado de incidencia se puede identificar que riesgo se debe mitigar con mayor prioridad. Finalmente se realizó un enfoque de mitigación para cada activo, donde se crearon grupos que indican la prioridad con el que deben ser tratados los posibles riesgos y las recomendaciones de control se deberían implementar.

La implementación de las recomendaciones que se dieron en el proyecto para cada activo de información queda a disposición del jefe del Departamento Tecnológico del GAD de San Pedro de Pelileo quien decidirá si la aplican inmediatamente.

ABSTRACT

In this research work, an IT Audit of the permit and collection processes of the Autonomous Decentralized Government of San Pedro de Pelileo, Tungurahua Province, was carried out with the objective of identifying flaws and establishing the necessary controls to guarantee the security and integrity of the information.

For the development of the present investigation, the OCTAVE methodology was used, which has eight phases, in which the risk measurement criteria were first established according to what the entity required, subsequently the identification of information assets was carried out. interact with the processes to be audited, for this purpose profiles were created for each information asset and their containers were identified. Then the different areas of concern were determined, which are basically the problems that could arise in the entity in relation to the management of information technologies, with this we proceeded to detail the scenarios of potential threats and created a tree of threats for each active, then proceeded to establish the consequences that could occur in the event that a threat is met, then qualitatively measured the degree to which the institution would be affected by each threat and according to the value and degree of incidence can be identify what risk should be mitigated with higher priority. Finally, a mitigation approach was carried out for each asset, where groups were created indicating the priority with which the possible risks should be treated and the control recommendations should be implemented.

The implementation of the recommendations that were given in the project for each information asset is at the disposal of the Head of the Technological Department of the GAD of San Pedro de Pelileo who will decide whether to apply it immediately.

INTRODUCCIÓN

El presente trabajo tiene como principal objetivo realizar una Auditoria Informática de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado de San Pedro de Pelileo, se lo efectúo mediante la aplicación de la metodología OCTAVE que ayuda a la identificación de las posibles vulnerabilidades y riesgos que podrían tener los activos de la institución; con anterioridad en esta entidad pública no se han aplicado ningún proyecto con la finalidad de auditar los procesos que se realizan en la institución.

La importancia de este proyecto radica en que se pudo realizar una valoración de los procesos y activos de TI de la institución, esto se llevó a cabo mediante la recolección de información con técnicas como la observación, entrevista y encuesta a quienes intervienen en los procesos. Con el análisis realizado se procedió a la aplicación de la metodología teniendo como resultado un plan de mitigación con recomendaciones relacionadas con un mejor uso de las Tecnologías de Información y propuestas para mejorar la seguridad e integridad de la información que se maneja internamente en la entidad pública.

El presente trabajo denominado "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA OCTAVE DE LOS PROCESOS DE RECAUDACIONES Y PERMISOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO (GAD) DE SAN PEDRO DE PELILEO.", consta de cinco capítulos que se detallan a continuación:

CAPÍTULO I "EL PROBLEMA". - identifica las necesidades de la entidad dentro de un contexto real para que pueda ser planteado en conformidad con la situación actual, definiendo alcance, justificación y objetivos a cumplir que servirán como guía en el transcurso del proyecto.

CAPÍTULO II "MARCO TEÓRICO". - contiene la recopilación de información teórica necesaria para comprender el problema y poder así sugerir una posible solución.

CAPÍTULO III "METODOLOGÍA". - describe las modalidades aplicadas de investigación, el entorno con el cual se va a trabajar y una breve descripción de la manera en cómo estará desarrollado el proyecto.

CAPÍTULO IV “DESARROLLO DE LA PROPUESTA”. - Presenta el desarrollo del portal web en conjunto con la metodología.

CAPÍTULO V “CONCLUSIONES Y RECOMENDACIONES”. - se dan a conocer las conclusiones y recomendaciones que surgieron una vez concluido el desarrollo del proyecto investigativo.

Finalmente, se incluye las referencias consultadas y se anexa la encuesta, entrevista, tablas de la auditoria.

CAPÍTULO 1: EL PROBLEMA

1.1 Tema:

Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo.

1.2 Planteamiento del problema

En la actualidad la dependencia de las Tecnología de Información (TI) ha ido en crecimiento constante; además, se han vuelto de gran utilidad en casi todos los sectores imaginables; van desde actividades cotidianas hasta la administración de grandes empresas. Es aquí donde se relaciona directamente con la gestión empresarial e institucional, los cuales siempre tendrán estándares, normas y lineamientos que deberán ser cumplidos. La auditoría informática nace para regular que las TI en la institución tengan un adecuado funcionamiento.

A nivel internacional un estudio de expertos en seguridad informática indica que hay un incremento en el interés de los atacantes informáticos en la información de las empresas enfocándose principalmente en datos de usuarios, planos, esquemas, documentos, etc. La mayor parte de esta se da desde el interior de la entidad siendo los propios empleados quienes realizan este delito, debido a que no se tiene un control y gestión adecuada de los recursos informáticos [1].

Un estudio realizado por el Banco Interamericano de Desarrollo y la Organización de Estados Americanos menciona que en Latinoamérica de cada cinco países cuatro no tiene un estrategia relacionado con ciberseguridad , por este motivo se plantea tener medidas de seguridad de información entre ellas la auditoría informática que ayuda a

las organizaciones a tener una mejor validación de datos, además se sugiere controlar que se cumpla las normas de calidad en lo que se tiene que ver con desarrollo, implantación, operación y mantenimiento de TI [2].

Las instituciones de Ecuador se van adaptando a los cambios tecnológicos y cada vez requiere tener un mejor desempeño organizacional que busca tener el mayor beneficio posible para la institución teniendo en cuenta los recursos disponibles y políticas de la misma

Los delitos informáticos en Ecuador se los responsabiliza en un 85% al descuido de los usuarios debido a que no se toman las precauciones al ingresar o utilizar los distintos tipos de sistemas informáticos, la mayor parte de delitos se dan en las provincias como son Pichincha, Guayas y Manabí, pero el resto de provincias no está excepto de sufrir este tipo de violación de seguridad de información [3].

Las auditorias informáticas se basan en la medición y control de riesgos de información, para ello se debe cumplir normas y estándares internacionales entre las más utilizadas tenemos ISO 27000, ITIL y COBIT, las tres están encaminadas en dar una mejor utilización a las TI; así tenemos que ISO 27000 hace un marco de referencia de segundad e integridad de la información, ITIL registra un mapeo de gestión de niveles de servicio de la TI y COBIT realiza un control de la información de TI [4].

Además de las normas y estándares para la auditoria informática se debe combinar con metodologías para la gestión de riesgos las más utilizadas son MAGERIT y OCTAVE, en lo que podemos destacar que OCTAVE se basa en una evaluación organización, un enfoque sobre prácticas de seguridad y puede ser autodirigido, mientras que MAGERIT aplica una evaluación de sistemas, enfoque sobre prácticas de tecnología y debe ser dirigido por expertos, la elección de la metodología depende del tipo de institución en la que se plantea aplicar la auditoria [5].

Octave es una metodología basada en el análisis de riesgos que consta de un conjunto de criterios con los cuales se desarrollan guías específicas de evaluación y administración de riesgos, hay que tener en cuenta que Octave se enfoca en la evaluación de riesgos de seguridad de la información, considerando personas, hardware, software, información y sistemas, para posteriormente proponer un plan de mitigación dentro de una organización. [6]

Actualmente el Gobierno Autónomo Descentralizado de San Pedro de Pelileo maneja varios procesos que hacen crecer la información, pero sin tomar en cuenta esta se vuelve susceptible a vulnerabilidades. También se debe tomar en cuenta que las TI no son aprovechadas en su totalidad ya que no se realiza una correcta evaluación de procesos que posteriormente afectan tanto a los trabajadores del GAD de Pelileo como a los ciudadanos que se acercan a realizar los trámites correspondientes a los distintos.

El GAD de San Pedro de Pelileo con anterioridad se han realizado auditorias informáticas, pero con el problema que no se ha hecho en la totalidad de departamentos y tampoco se ha puesto énfasis en la seguridad e integridad de la información, por lo que no han tenido cambios representativos en el tratamiento de información [7].

Por lo tanto, el problema en definitiva radica en que no existe una evaluación de procesos correcta en lo que a sistemas tecnológicos se refiere y se desconoce su situación a nivel de seguridad informática, por lo tanto, no se toman decisiones y correctivos que garanticen la integridad de la información.

1.3 Delimitación

Área académica: Administrativas Informáticas

Línea de investigación: Administración de recursos

Sublíneas de investigación: Auditorias Informática

1.3.1 Espacial

La presente investigación se realizará en el Gobierno Autónomo Descentralizado del San Pedro de Pelileo

1.3.2 Temporal

La presente investigación se desarrollará en el Periodo Académico septiembre 2018-febrero 2019

1.4 Justificación

La mayor cantidad de empresas y organizaciones tanto públicas como privadas no ponen énfasis en lo que se refiere a la seguridad de la información que a corto y largo plazo pueden causar pérdidas para estas entidades, por lo que no se asignan suficientes recursos.

Los distintos tipos de procesos que se llevan a cabo en el Gobierno Autónomo Descentralizado del San Pedro de Pelileo tales como extensión de permisos de funcionamiento, permiso de uso de suelos, cobros de agua potable y pagos de impuestos prediales generan gran cantidad de información que es manipulada por medios tecnológicos sin embargo no toda la información es tratada correctamente.

La investigación es factible debido a que existe el conocimiento necesario para la realización del presente estudio aprovechando la información que se podrá obtener de la entidad pública ya que existe total apertura por parte de esta y optimizando recursos disponibles.

La entidad pública será la principal beneficiaria ya que obtendrá un plan de mitigación en el cual se expondrán como mejorar las prácticas para reducir vulnerabilidades de información en lo que tiene que ver con las TI.

El financiamiento del estudio será por parte del investigador.

1.5 Objetivos

1.5.1 Objetivo General

Realizar una Auditoría Informática de procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado de San Pedro de Pelileo aplicando la metodología OCTAVE.

1.5.2 Objetivos Específicos

-Analizar la situación actual de la Institución centrándose en las Tecnologías de la Información que utilizan.

-Aplicar la metodología OCTAVE para realizar la Auditoría Informática de procesos en el GAD de San Pedro de Pelileo.

-Emitir recomendaciones que permitan reducir riesgos en los procesos informáticos de la Institución y asegurar una mayor integridad de la información.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Antecedentes investigativos

En el Gobierno Autónomo Descentralizado de San Pedro de Pelileo no se aplicado ningún proyecto relacionado con la Auditoria Informática de los distintos procesos que tiene la entidad pública.

En la Universidad Distrital Francisco José De Caldas de Colombia, Sandra Torres y Jeimy Lorena en su proyecto " Modelo de Gestión de Riesgos Aplicando Metodología Octave en entidades del Sector Fiduciario", en el 2017; menciona que el realizar una gestión de riesgos en una entidad permite identificar, mitigar y monitorear los riesgo que pueden existir, para posteriormente tratar de reducir las vulnerabilidades y amenazas existentes obviamente todo con referencia a las Tecnologías de la Información [8].

En la Universidad de Cuenca, Paul Crespo en su proyecto "Metodología de Seguridad de la Información para la Gestión del Riesgo Informático Aplicable A Mpymes", en el 2016; da a conocer que la información es lo más valioso que puede tener una organización ya que con ella se puede crear ventajas competitivas pero al no tener conocimiento suficiente para proteger y manejar dicha información se quedan estancados en un solo punto para ello surgieron las distintas metodologías que ayudan a gestionar el riesgo informático con lo que ayuda en gran medida a identificación, corrección y manejo amenazas en la información [9].

En la Universidad de Cuenca, el Ing. Franklin Arévalo en su proyecto de postgrado "Elaboración y plan de implementación de políticas de Seguridad de la Información aplicadas a una Empresa Industrial de Alimentos", en el 2017; indica que en empresas industriales hay una cantidad considerable de información crítica de los distintos procesos que se realizan por lo que debe ser resguardada contra posibles riesgos a los

que pueden ser susceptibles; para ello es necesario establecer proyectos de seguridad que vendrían a ser las auditorias informáticas que ofrecen una guía para la mejora del manejo de información. Además, se menciona que para la aplicación de cualquier tipo de estándar se debe acoplar a las políticas internas de la entidad [10].

En la Universidad Regional Autónoma de los Andes "UNIANDES", la Ing. Andrea Mejía en su proyecto de postgrado "Auditoría de Gestión Informática en el Área de las Tecnologías de la Información para el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón La Concordia", en el 2017; menciona que mediante la aplicación de la Auditoria informática verifico el cumplimiento de las funciones asignadas a los funcionarios, empleados y usuarios de Área de Tecnología de esta entidad, y que se pudo determinar correctivos necesarios al uso de la información y la administración de recursos tecnológicos promoviendo una gestión adecuada [11].

En la Escuela Superior Politécnica de Chimborazo, Fanny Guevara y Gabriela Torres en su proyecto "Auditoria Informática al GAD Municipal de la Ciudad de Riobamba, Provincia de Chimborazo del Período 2014", en el 2016; recomiendan la elaboración de indicadores de eficiencia, eficacia y seguridad del área informática para con estos identificar los distintos riesgos y vulnerabilidades que están presentes en la institución para posteriormente proceder a determinar las medidas que se deben tomar para reducir lo que puede afectar a la información de la institución [12].

En la Universidad Técnica de Ambato, Jorge Ulloa en su proyecto "Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate", en el 2017; recomienda realizar una documentación de los distintos procesos tecnológicos de la entidad con el fin de evitar perdida de información debido a las vulnerabilidades que se encontraron mediante la auditoria, además también menciona que sería necesario realizar capacitaciones a los usuarios que manejan las Tecnologías de Información para que el desempeño de estos mejore de acuerdo con las necesidades de la institución [13].

En la Universidad Técnica de Ambato, Yajaira Carcelén en su proyecto "Auditoria Informática Mediante la aplicación de la Metodología COBIT (Control Objectives for Information and Related Technology) en la entidad I COACH SERVICIOS Consulting & Training Cia. Ltda.", en el 2015; indica que mediante la auditoria se

puede identificar si los procesos que se desarrollan en una empresa son estructurados, además al realizar el análisis de situación se puede verificar si existen políticas o procedimientos que no estén correctamente optimizados siendo perjudiciales para la entidad ya que se desperdician recursos. Ya identificados las vulnerabilidades se podrían aplicar planes de acción con respecto a los distintos procesos con el objetivo de mejor la eficiencia y optimizar los recursos que se dispone [14].

2.2 Fundamentación teórica

2.2.1 Auditoría

Es una revisión sistemática y exhaustiva con el fin de obtener evidencias y verificar la veracidad de información, estados, registros y operaciones de una entidad [15].

La Auditoria busca verificar que la información financiera, administrativa, tecnológica y operacional que se genera es confiable, veraz y oportuna. Es revisar que los hechos, fenómenos y operaciones se den en la forma en que fueron planteados, que las políticas y procedimientos establecidos se han observado y respetado. Es evaluar la forma en que se administra y opera para aprovechar al máximo los recursos [16].

2.2.2 Tipos de Auditoría

La auditoría puede clasificar según el origen puede ser de carácter interna cuando es realizado por los miembros de la entidad o externa cuando se realiza por un auditor ajeno a la institución y por lo general especialista en el tema.

Pero también se puede clasificar según el área en donde se realiza como se puede apreciar en la Tabla 1.

Tipo de Auditoria	Descripción
Auditoría Financiera	Examina los estados financieros del objeto contable, a fin de emitir un informe técnico y profesional que funde la claridad en las operaciones financieras realizadas por el mismo en un periodo determinado.
Auditoría Administrativa	Revisa y evalúa los métodos y procedimientos del proceso administrativo de un ente económico, a fin de asegurar el cumplimiento de los planes, políticas, leyes y reglamentaciones, además de medir el impacto en la estructura de la organización y su productividad.

Tipo de Auditoria	Descripción
Auditoría Operacional	Evalúa la empresa y su gestión, a fin de proponer mejoras para aumentar la eficiencia y eficacia productividad. Se realiza a solicitud de la dirección, pero es llevada a cabo por un auditor externo.
Auditoría Gubernamental	Es una auditoría pública, se lleva a cabo por un ente gubernamental con las competencias de ley para hacerlo, en algunos países el encargado de llevarla es el tribunal de cuentas.
Auditoría Integral	Evalúa toda la información posible y útil para emitir un informe certero y completo acerca del cumplimiento ye desempeño de la organización, incluyendo estructura organizacional, información financiera, procedimientos de control interno, objetivos y acatamiento de leyes.
Auditoría Informática o de Sistemas	Es la evaluación exhaustiva mediante actividades, técnicas y procedimientos, con el fin de analizar, verificar y forjar recomendaciones relativas a la planificación, seguridad y eficacia de la asistencia informática dentro de la empresa, en busca del mejoramiento del mismo.
Auditoría Contable	Es la revisión de la situación económica de la empresa, verifica todas las cuentas bien sean por pagar, por cobrar, gastos y ventas, realizada por un auditor externo.

Tabla 1 Tipos de Auditoria

Fuente: Elaboración propia a partir de [17]

2.2.3 Auditoria Informática

La Auditoría informática hace referencia a realizar una verificación de recursos informáticos de una entidad para posteriormente dar un informe sobre la situación en que se encuentra la administración y utilización dichos recursos [18].

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, manteniendo la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos [19].

2.2.3.1 Tipos de Auditoría informática

Auditoria	Descripción	Revisión
Auditoria Informática de Explotación	La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos magnéticos para otros informáticos, órdenes automatizadas para lanzar o modificar procesos, etc.	- Control de entrada de datos - Planificación y Recepción de Aplicaciones - Operadores de Centros de Cómputos -Centro de Control de Red y Centro de Diagnosis
Auditoria Informática de Sistemas	Se ocupa de analizar la actividad propia de lo que se conoce como "Técnica de Sistemas" en todas sus facetas. En la actualidad, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de "Sistemas".	- Sistemas Operativos - Software Básico -Software de Teleproceso -Optimización de los Sistemas y Subsistemas -Administración de Base de Datos -Investigación y desarrollo
Auditoria Informática de Comunicaciones	Una auditoria en redes es un mecanismo de prueba de una red informática, con el fin de evaluar el desempeño, seguridad de la misma, logrando así la utilización más eficiente y segura de la red.	-Estructura física/hardware -Estructura lógica/software del sistema.
Auditoria Informática de Desarrollo de Proyectos	El área de Desarrollo de Proyectos o de Aplicaciones es objeto frecuente de la Auditoria informática. Indicando inmediatamente que la función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones.	- Revisión de las metodologías utilizadas - Control Interno de las Aplicaciones - Control de Procesos y Ejecuciones de Programas Críticos - Satisfacción de Usuarios - Control de Procesos y Ejecuciones de Programas Críticos

Auditoria	Descripción	Revisión
Auditoria Informática de Seguridad	El auditor de seguridad informática comprueba que las medidas de seguridad y control de los sistemas informáticos se adecúan a la normativa que se ha desarrollado para la protección de los datos; identifica las deficiencias, y propone medidas correctoras o complementarias.	- Analizar el nivel de seguridad del sistema informático utilizado en la empresa - Servidores web -Correo electrónico -FTP -Conexiones VPN

Tabla 2 Tipos de Auditoría informática

Fuente: Elaboración propia a partir de [20]

2.2.3.2 Objetivos de una Auditoria Informática.

- Saber cuál es la situación verdadera y precisa de la organización en general o de una parte en particular.
- Analizar eficiencia de los Sistemas Informáticos.
- Verificar cumplimiento de la Normativa en este ámbito.
- Revisar la eficaz gestión de los recursos informáticos.
- Mejorar las posibles incidencias que pueda presentar un sistema informático
- Identificar posibles fraudes que estén ocurriendo en la organización.
- Corroborar la legitimidad de los productos y/o servicios.
- Encontrar posibles fallas técnicas.
- Analizar si el trabajo de la organización es eficiente [21].

Beneficios de la Auditoria Informática

- Mejora la imagen pública, debido a que hay una mejor organización interna.
- Utiliza la información analizada para dar soluciones concretas de rentabilidad en el trabajo, como adquisición de nuevos equipos, componentes o compras de licencias o instalación de software.
- Da consejos sobre una utilización más eficiente de los recursos, lo que evita errores de gestión y por lo tanto ahorra tiempo y dinero.
- Permite poner en marcha mecanismos de protección ante los riesgos derivados del uso de las nuevas tecnologías
- Mejora las relaciones entre departamentos, al proponer sinergias en cuestiones informáticas para hacer más rentable la comunicación entre diferentes trabajadores [18].

2.2.4 OCTAVE (Evaluación de amenazas, activos y vulnerabilidades operacionalmente críticas)

OCTAVE se centra en el estudio de riesgos organizacionales y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto como los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa en el día a día. En OCTAVE se considera que, con el fin de que una organización pueda cumplir su misión, los empleados a todo nivel necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos; para ello, es fundamental que en la evaluación estén directamente involucradas personas de diferente nivel de la organización [22].

OCTAVE se basa en los riesgos y la planeación de seguridad, al ser un proceso auto dirigido hace que las personas de la entidad además de participar en la evaluación se responsabilizan en hacer que se establezca la estrategia de seguridad [23].

Octave realiza una evaluación de riesgos para posteriormente proponer un plan de mitigación en el interior de la organización, se enfoca básicamente en concientizar a los miembros de la organización a pensar de una manera diferente con respecto a la seguridad de la información ya que no es un asunto solamente técnico [24].

Los procesos que realiza la metodología inician con la evaluación de activos relacionados con la información que al ser analizados se estima el nivel de organización con el que cuenta para posteriormente tomar decisiones basada en los riesgos potenciales encontrados con el fin de proteger la información crítica y beneficiar a la entidad mediante la posibilidad de crear una estrategia de contingencia para la reducción de riesgos de seguridad de información [25].

OCTAVE está compuesta por tres fases:

Visión de organización: Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.

Visión tecnológica: se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.

Planificación de las medidas y reducción de los riesgos: se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos, como se muestra en la Figura 1 y Tabla 3.

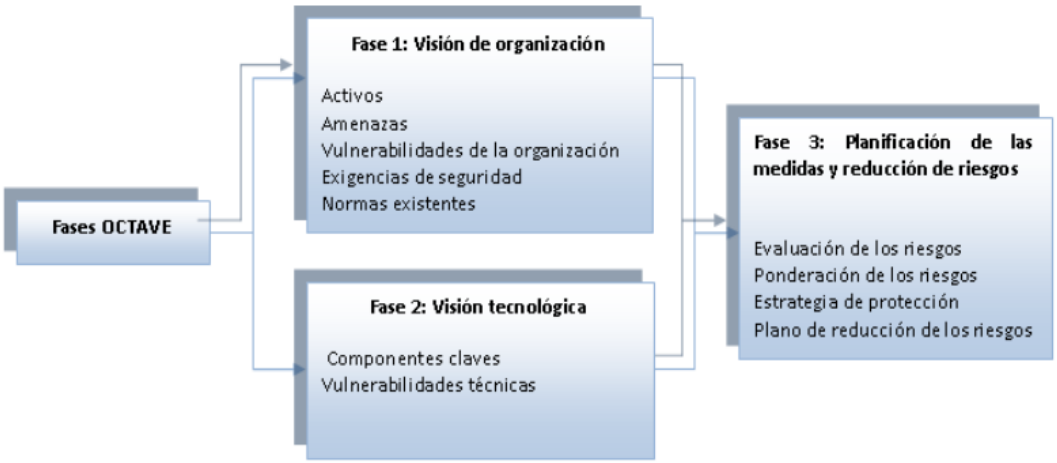


Fig. 1Fases y elementos de OCTAVE

Fuente: [26]

Fases y procesos de la Metodología OCTAVE		
Fase	**Proceso**	**Descripción**
1.-Visión de la organización	1.- Identificar el conocimiento de los altos directivos	En este proceso se recopila información de los principales activos de la organización, los niveles de seguridad y los motivos de preocupación por esos activos, así como también las estrategias actuales de protección y las vulnerabilidades de la organización. Los participantes de este nivel son los altos directivos de la organización.

Fases y procesos de la Metodología OCTAVE		
Fase	**Proceso**	**Descripción**
1.-Visión de la organización	2.- Identificar el conocimiento de los directivos de áreas operativas	Este proceso tiene como objetivo recopilar información a nivel operativo, es decir, de los encargados operacionales de los activos importantes de la organización, de igual forma que en el anterior proceso se identificará los requisitos de seguridad y los motivos de preocupación por esos activos. Los participantes de este nivel son los encargados de las aéreas operativas.
	3.- Identificar el conocimiento del personal	En este nivel se recopila información de miembros del personal sobre activos importantes de la organización, requisitos de seguridad y motivos de preocupación por esos activos, estrategias actuales de la protección y vulnerabilidades de la organización. En este nivel hay dos tipos de participantes: el personal de planta y el personal del departamento de Tecnología de Información.

Fases y procesos de la Metodología OCTAVE		
Fase	**Proceso**	**Descripción**
1.-Visión de la organización	4.- Crear perfiles de amenaza	En este proceso el equipo de análisis analiza la información obtenida durante los procesos 1 al 3, en donde se seleccionan 5 activos críticos sobre los cuales se definen los requisitos y las amenazas de seguridad para esos activos.
2.-Visión Tecnológica	5.-Identificar componentes claves	En este nivel para cada activo crítico encontrado hay que identificar los componentes claves que se deben evaluar para las vulnerabilidades de la tecnología. El equipo de análisis realiza esta actividad, con ayuda del personal de TI, según la necesidad.
	6.-Evaluación de componentes seleccionados	Identificar las principales vulnerabilidades de los componentes críticos. En este nivel el equipo del análisis y los miembros de equipo suplementarios evalúan cada uno de los componentes de la infraestructura de tecnología, identificando las vulnerabilidades de estos. Aquí se necesita la ayuda de herramientas de evaluación de vulnerabilidades.

Fases y procesos de la Metodología OCTAVE		
Fase	**Proceso**	**Descripción**
3.-Planificación de las medidas y reducción de riesgos	7.- Realizar un análisis de riesgos	Identificar los riesgos que se podrían dar sobre los activos críticos de una organización. Para realizar este proceso se utiliza la información recopilada. Este proceso utiliza la información de los procesos 1 al 6 para crear los perfiles de riesgo para los activos críticos, en donde se define cada una de las descripciones de los impactos encontrados, se crean los criterios de evaluación, y al final se evalúan los resultados de cada amenaza contra los criterios. Este proceso es realizado por el equipo del análisis, en colaboración con personal suplementario (encargado operacional del área) según lo necesitado.
	8.- Desarrollo de estrategias de protección	Se debe definir una serie de acciones, estrategias y planes para proteger los activos críticos, los cuales deberán ser estudiados y aprobados para su ejecución

Tabla 3 Fases y procesos de la Metodología OCTAVE

Fuente: Elaboración propia a partir de [26].

2.2.5 Gestión de Procesos TI

Los Procesos de TI estandarizan todas las actividades de la empresa relacionadas con la tecnología de la información, lo que las lleva a un alto nivel de calidad y excelencia.

Con los procesos de TI, los servicios tienen la entrega garantizada, independientemente de quién los ejecuta.

Los Procesos de TI se deben considerar como una parte integral y esencial de la gestión de procesos de negocio y, por lo tanto, recibir recursos e inversiones frecuentes para que se puedan mejorar y optimizados continuamente, lo que contribuye al desarrollo y crecimiento de los negocios de la organización [27].

La gestión de TI asegura que todos los recursos tecnológicos y los empleados asociados son utilizados correctamente y de una manera que proporciona valor para la organización. La gestión de TI permite a una organización optimizar los recursos y la dotación de personal, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas. Las personas que trabajan en la gestión de TI también deben demostrar habilidades en áreas generales de gestión como liderazgo, planificación estratégica y asignación de recursos.

2.2.6 Seguridad de la Información

La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa. Principalmente este tipo de sistemas se basan en las nuevas tecnologías, por tanto, la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán acceso usuarios autorizados. Por otro lado, tampoco se podrán hacer modificaciones en la información a no ser que sea de la mano de los usuarios que tengan los permisos correspondientes [28].

La seguridad de la información responde a las siguientes:

- Critica. -debido a que es indispensable para que la entidad realice sus actividades sin tener que asumir demasiado riesgo.
- Valiosa. -debido a que los datos son esenciales para el funcionamiento del negocio.
- Sensible. – debido a que solo personas autorizadas tendrán acceso a los datos.

2.2.6.1 Objetivo y aspectos principales de la Seguridad de la Información

El principal objetivo de la seguridad de la información es proteger los datos de la empresa, para ello internamente se deberán tener estrategias, controles y políticas de seguridad; siempre con el fin de asegurar tres aspectos fundamentales como son la

confidencialidad, disponibilidad e integridad de la información, que se detalla en la Tabla 4.

Aspecto de Seguridad de Información	Descripción
Confidencialidad	A través de ella la seguridad de la información garantiza que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información.
Disponibilidad	Toda la información que se encuentre recogida en el sistema tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento que ellos necesiten acceder a ella.
Integridad	Para que el sistema sea veraz los datos no deben manipularse. Así se garantiza que la información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

Tabla 4Aspectos principales de la Seguridad de la Información

Fuente: Elaboración propia a partir de [28].

2.2.7 Análisis y Gestión de Riesgos de TI

Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo [29].

2.2.7.1 Gestión de Riesgos de TI en forma General

En forma general se puede identificar 4 fases para realizar un Gestión de Riesgo de TI, como se muestra en la Tabla 5.

Fase	Descripción
Análisis	Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
Clasificación	Determina si los riesgos encontrados y los riesgos restantes son aceptables.
Reducción	Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas
Control	Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Tabla 5 Gestión de Riesgos de TI en forma General
Fuente: Elaboración propia a partir de [30].

2.3 Propuesta de solución

Realizar una auditoría informática aplicando la Metodología OCTAVE, para el análisis de riesgos y recomendaciones estratégicas de Seguridad de los elementos de Tecnologías de Información, en los procesos de recaudaciones y permisos del Gobierno Autónomo Descentralizado de San Pedro de Pelileo.

CAPÍTULO 3: METODOLOGÍA

3.1 Modalidad de la investigación

3.1.1 Investigación Bibliográfica- Documental

Se utilizó la investigación bibliográfica o documental que permitió conocer, comparar, profundizar y deducir diferentes enfoques, teorías, conceptualizaciones y criterios de diversos autores sobre la cuestión determinada basándose en documentos como fuentes primarias, en libros, artículos científicos, repositorios, tesis de grado que proporcionaron la información que se requería para tener una idea clara del problema objeto de estudio.

3.1.2 Investigación de campo

La investigación de campo proporción información primaria sobre los procesos que se realizan en el Gobierno Autónomo Descentralizado de San Pedro de Pelileo; para ello acudimos a las instalaciones de la entidad pública a analizar cómo se realizan los distintos procesos, de esta manera nos involucramos directamente en la obtención de la información.

3.1.3 Investigación Aplicada

En virtud de que en el presente estudio se estableció claramente el problema y es conocido por el investigador, se utilizó la investigación para generar soluciones a requerimientos específicos de un cuestionamiento particular en el ámbito de los procesos de TI.

3.2 Población y muestra

Por la característica de las investigaciones no se requieren población y muestra.

3.3 Recolección de información

Para la investigación se obtuvo la información mediante técnicas tales como la observación que se realizó en las distintas oficinas del GAD de San Pedro de Pelileo en donde se planifico realizar la auditoria informática de los distintos procesos que se realiza en la entidad. Además, se efectuó una entrevista al encargado del Departamento Tecnológico con el fin de enterarnos de la situación en que se encuentra la administración de los sistemas y la utilización de las TI.

3.4 Procesamiento y análisis de datos

La información obtenida se organizó, representó y analizó, presentando los resultados en porcentajes y diagramas que permitirán establecer en forma gráfica la realidad del problema planteado y la necesidad de un cambio o mejoramiento de la situación existente, a través de herramientas de análisis.

3.5 Desarrollo del proyecto

En el desarrollo del proyecto se emplearon los siguientes pasos:

- Análisis de la situación actual de la entidad pública.
- Plantear alcance de la auditoría informática
- Establecer recursos para la realización de la auditoría.
- Elaboración del plan de auditoría.
- Identificación del nivel de conocimiento de los miembros de la entidad.
- Selección y creación de Perfiles de Amenaza
- Identificación y evaluación de vulnerabilidades de componentes críticos
- Análisis de riesgos de los activos de TI.
- Creación de estrategias de Protección
- Elaboración del informe final

CAPITULO 4: DESARROLLO DE LA PROPUESTA

4.1 Análisis de la situacional actual

4.1.1 Antecedentes

Pelileo fue un pequeño pueblo fundado por el español Antonio Clavijo en el año de 1570 y mediante decreto expedido por el Gobierno Provisorio el 3 de Julio de 1860, se creó el Cantón Pelileo y elevó al estatus de Provincia a Tungurahua.

Mediante decreto particular dictado por el Jefe Civil y Militar, don Antonio Muñoz, con fecha 22 de julio de 1860, en el artículo 3 menciona que por primera vez y en razón de que no estar establecido el orden municipal, la Jefatura Superior otorgaría los nombramientos de Jefe Político, Alcalde Municipal, Concejeros, Procurador Síndico y más empleados del Cantón, los mismos que serían posesionados mediante juramento ante el Gobernador de la Provincia. Fue así como Pelileo inició sus actividades municipales el 31 de Julio de mismo año. [31]

El Gobierno Autónomo Descentralizado del cantón San Pedro de Pelileo actualmente se rige de acuerdo con lo dispuesto por la Constitución de la República del Ecuador, pero además es una entidad de gobierno seccional, es decir, que trabaja conjuntamente con la población para cubrir las necesidades y aspiraciones de la comunidad de forma autónoma e independiente del gobierno central.

Esta institución pública esta administrada por dos poderes que son el ejecutivo y el legislativo cada uno de ellos representado por dignidades elegidas por democráticamente por voto popular, el poder ejecutivo es representado por el señor Alcalde del cantón y el legislativo por los miembros del Consejo Cantonal. [32]

El GAD de San Pedro de Pelileo ha tenido grandes cambios estructurales con la finalidad de dar una mejor atención a la comunidad, entre ellos tenemos los recursos informáticos que son los principales ya que mediante estos se trata agilitar y automatizar los procesos de la institución para realizarlos en un menor tiempo.

El GAD municipal del cantón Pelileo contaba con sistemas informáticos que no satisfacían las necesidades de la institución, pero mediante varios proyectos han ido desarrollando sistemas a medida y por lo tanto reduciendo las deficiencias, aunque todavía hay varias cosas que se pueden mejorar.

4.1.2 Competencias Exclusivas de GAD de San Pedro de Pelileo

a. Planificar, junto con otras instituciones del sector público y actores de la sociedad, el desarrollo cantonal y formular los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, provincial y parroquial, con el fin de regular el uso y la ocupación del suelo urbano y rural, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad;

b. Ejercer el control sobre el uso y ocupación del suelo en el cantón;

c. Planificar, construir y mantener la vialidad urbana;

d. Prestar los servicios públicos de agua potable, alcantarillado, depuración de aguas residuales, manejo de desechos sólidos, actividades de saneamiento ambiental y aquellos que establezca la ley;

e. Crear, modificar, exonerar o suprimir mediante ordenanzas, tasas, tarifas y contribuciones especiales de mejoras;

f. Planificar, regular y controlar el tránsito y el transporte terrestre dentro de su circunscripción cantonal;

g. Planificar, construir y mantener la infraestructura física y los equipamientos de salud y educación, así como los espacios públicos destinados al desarrollo social, cultural y deportivo, de acuerdo con la ley;

h. Preservar, mantener y difundir el patrimonio arquitectónico, cultural y natural del cantón y construir los espacios públicos para estos fines;

i. Elaborar y administrar los catastros inmobiliarios urbanos y rurales;

j. Delimitar, regular, autorizar y controlar el uso de las playas de mar, riberas y lechos de ríos, lagos y lagunas, sin perjuicio de las limitaciones que establezca la ley;

k. Preservar y garantizar el acceso efectivo de las personas al uso de las playas de mar, riberas de ríos, lagos y lagunas;

l. Regular, autorizar y controlar la explotación de materiales áridos y pétreos, que se encuentren en los lechos de los ríos, lagos, playas de mar y canteras;

m. Gestionar los servicios de prevención, protección, socorro y extinción de incendios; y

n. Gestionar la cooperación internacional para el cumplimiento de sus competencias [32].

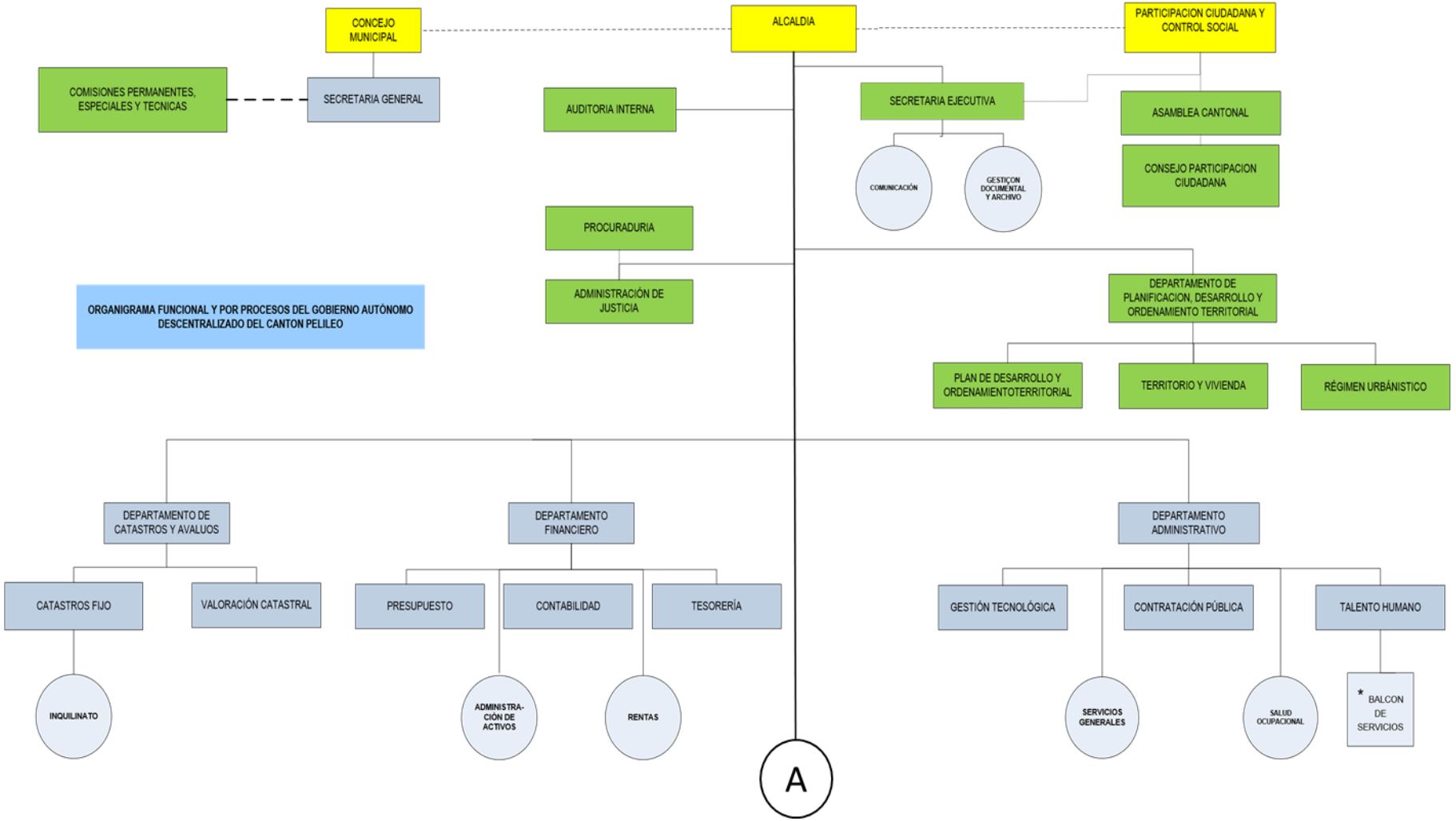
4.1.3 Estructura organizacional

4.1.3.1 Niveles Organizacionales

El GAD de San Pedro de Pelileo está conformado por 4 niveles:

- Nivel Directivo
- Nivel Operativo
- Nivel Desconcentrados
- Nivel de Apoyo

4.1.3.2 Organigrama Institucional



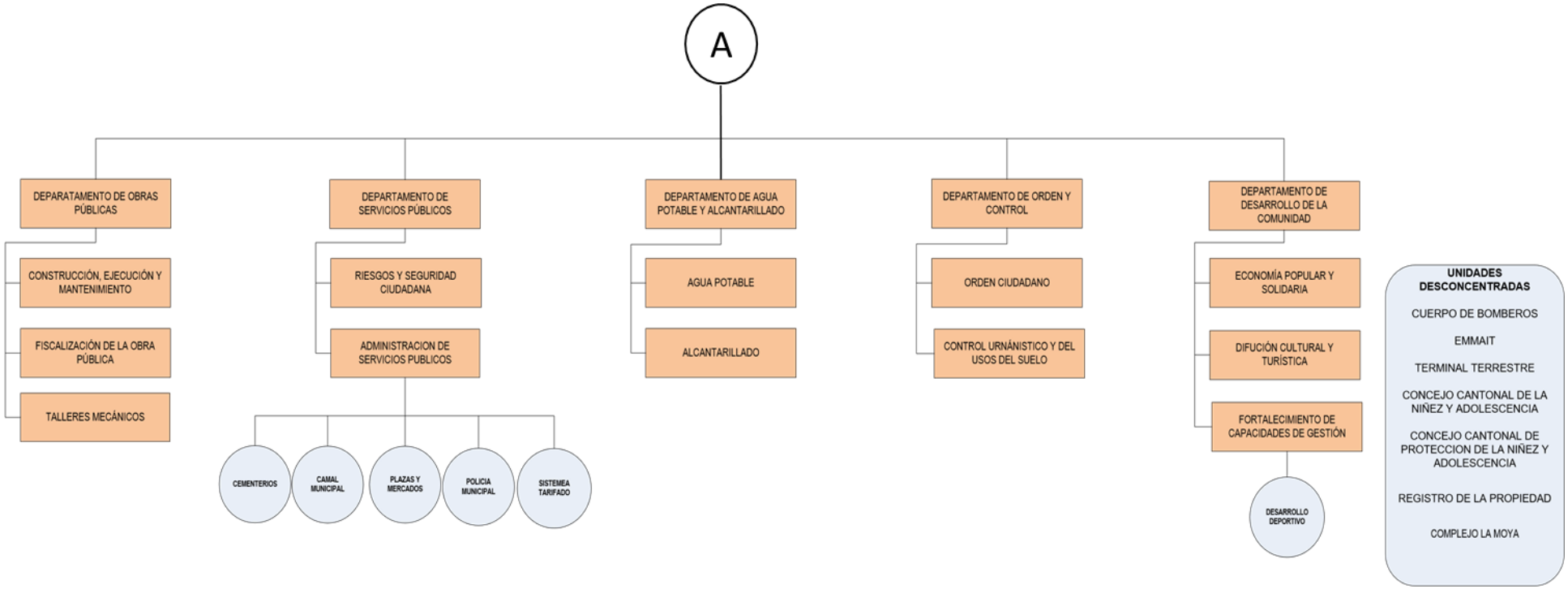


Fig. 2 Organigrama del GAD de San Pedro de Pelileo

Fuente: [33]

4.1.4 Direccionamiento Estratégico

El Gobierno Autónomo Descentralizado de San Pedro de Pelileo tiene dentro de su direccionamiento estratégico los siguientes elementos; como se muestra en la Tabla 6.

Direccionamiento Estratégico del GAD Pelileo	
Misión	Mejorar la calidad de vida de los habitantes del Cantón Pelileo, con una cuidadosa planificación, regulación y entrega de servicios e infraestructura pública.
Visión	Ser un gobierno participativo, ejemplo de trabajo e integridad, generador de oportunidades, y garante de derechos de los ciudadanos, del medio ambiente y del patrimonio cantonal.
Fines	• El desarrollo equitativo y solidario mediante el fortalecimiento del proceso de autonomías y descentralización; • La garantía, sin discriminación alguna y en los términos previstos en la Constitución de la República, de la plena vigencia y el efectivo goce de los derechos individuales y colectivos constitucionales y de aquellos contemplados en los instrumentos internacionales; • El fortalecimiento de la unidad nacional en la diversidad; • La recuperación y conservación de la naturaleza y el mantenimiento de un ambiente sostenible y sustentable; • La protección y promoción de la diversidad cultural y el respeto a sus espacios de generación e intercambio; la recuperación, preservación y desarrollo de la memoria social y el patrimonio cultural; • La obtención de un hábitat seguro y saludable para los ciudadanos y la garantía de su derecho a la vivienda en el ámbito de sus respectivas competencias; • El desarrollo planificado participativamente para transformar la realidad y el impulso de la economía popular y solidaria con el propósito de erradicar la pobreza, distribuir equitativamente los recursos y la riqueza, y alcanzar el buen vivir; • La generación de condiciones que aseguren los derechos y principios reconocidos en la Constitución a través de la creación y funcionamiento de sistemas de protección integral de sus habitantes

Direccionamiento Estratégico del GAD Pelileo	
Principios	• Honradez • Responsabilidad social • Justicia y equidad • Respeto y pluralismo • Protección al medio ambiente • Eficiencia y eficacia • Trabajo en equipo Participación.
Políticas	• Garantizar el uso eficiente de los recursos institucionales bajo principios de seguridad, eficiencia, sostenibilidad y responsabilidad en función de los estándares del ciudadano • Asegurar la diversidad de funciones y de las operaciones institucionales; y, canalizar los recursos hacia la inversión y gasto social prioritario • Propender a la universalización de las operaciones expandiendo la cobertura a todo el Cantón, procurando compatibilidad entre los fondos institucionales, las transferencias y la inversión con el servicio y obra pública. • Promover condiciones competitivas dentro de la dinámica productiva y comercial del Cantón. • Garantizar transparencia y eficiencia en la gestión del Gobierno Municipal, incorporando mecanismos de evaluación y rendición de cuentas, respetando la aplicación de normas, manuales y resoluciones. • Instrumentar mecanismos que permitan mitigar el riesgo en las operaciones de inversión pública municipal. • Asegurar el cumplimiento de los procesos operativos a través del seguimiento y acompañamiento.

Tabla 6 Direccionamiento Estratégico del GAD Pelileo
Fuente: Elaboración propia a partir [32] y [34].

4.1.5 Procesos institucionales en su entorno

4.1.5.1 Mapa de Procesos del GAD Municipal de San Pedro de Pelileo

El Municipio de Pelileo tiene variedad de procesos enfocados a satisfacer necesidades de los ciudadanos del cantón, en la Figura 3 se muestra el tipo de proceso y la distribución que este tiene.

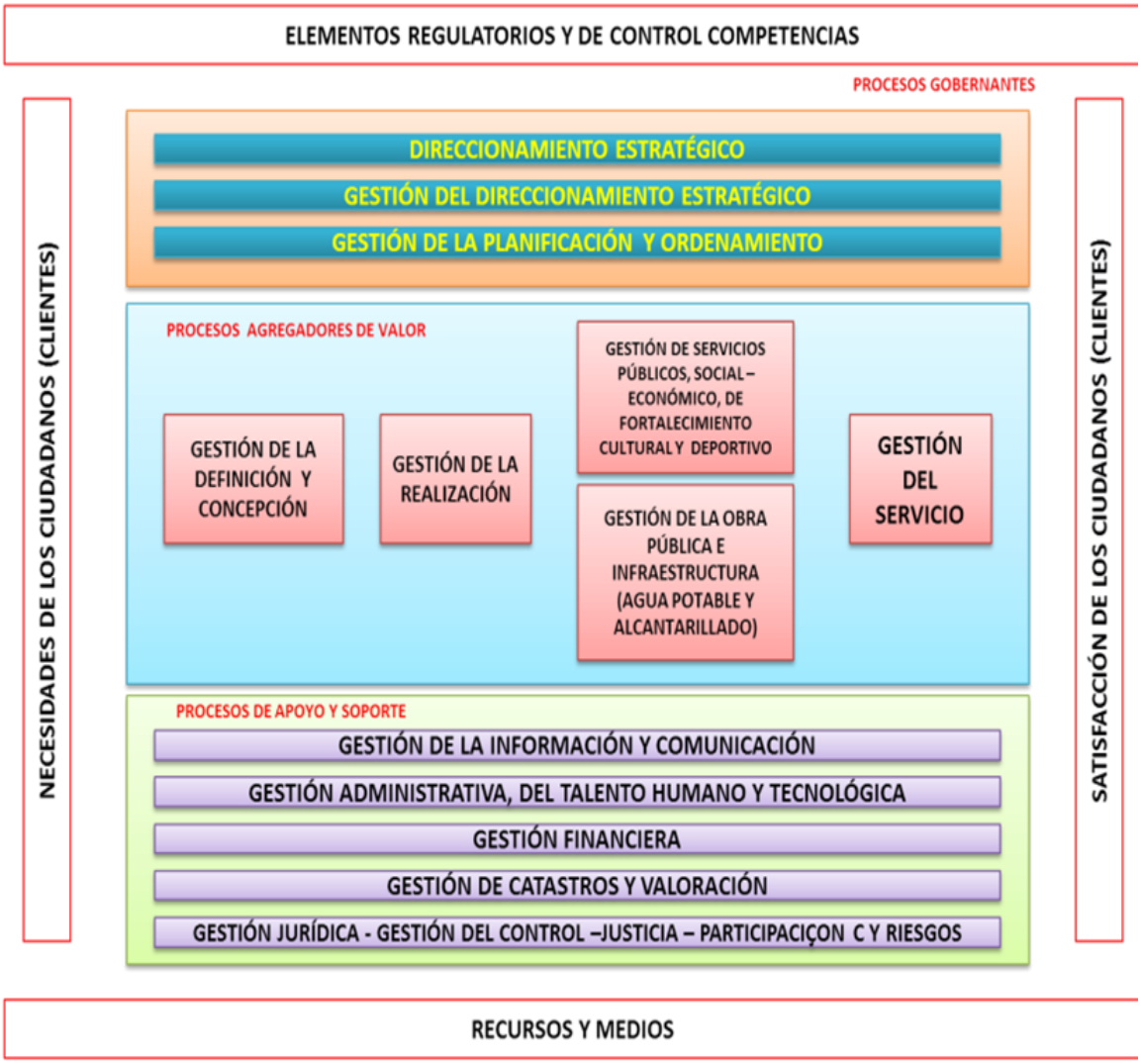


Fig. 3 Mapa de Procesos del GAD de San Pedro de Pelileo
Fuente: Recursos Humanos del GAD de San Pedro de Pelileo.

4.1.5.2 Análisis de procesos auditados en el GAD de San Pedro de Pelileo

En el GAD de San Pedro de Pelileo se realiza gran cantidad de procesos, pero por petición del del tutor institucional se centró en los procesos de recaudaciones y permisos.

Teniendo como resultado los siguientes procesos:

- Permisos de funcionamiento
- Cobro de impuestos
- Permisos de uso de suelos.
- Cobro de agua potable

Estos procesos poseen un funcionamiento similar teniendo como principal función la recaudación de ingresos para la entidad y se engloban en un solo sistema por lo que el jefe de Departamento Tecnológico solicitó que se audite los activos que intervienen en estos procesos, como alcance de la Auditoria informática.

Se realizó diagramas de flujo de los procesos que permitieron apreciar el funcionamiento secuencial que estos tienen; la información obtenida para realizar los diagramas fue mediante la observación y explicación de los empleados del municipio que realizar estos procesos.

Proceso 1: Cobro de impuestos

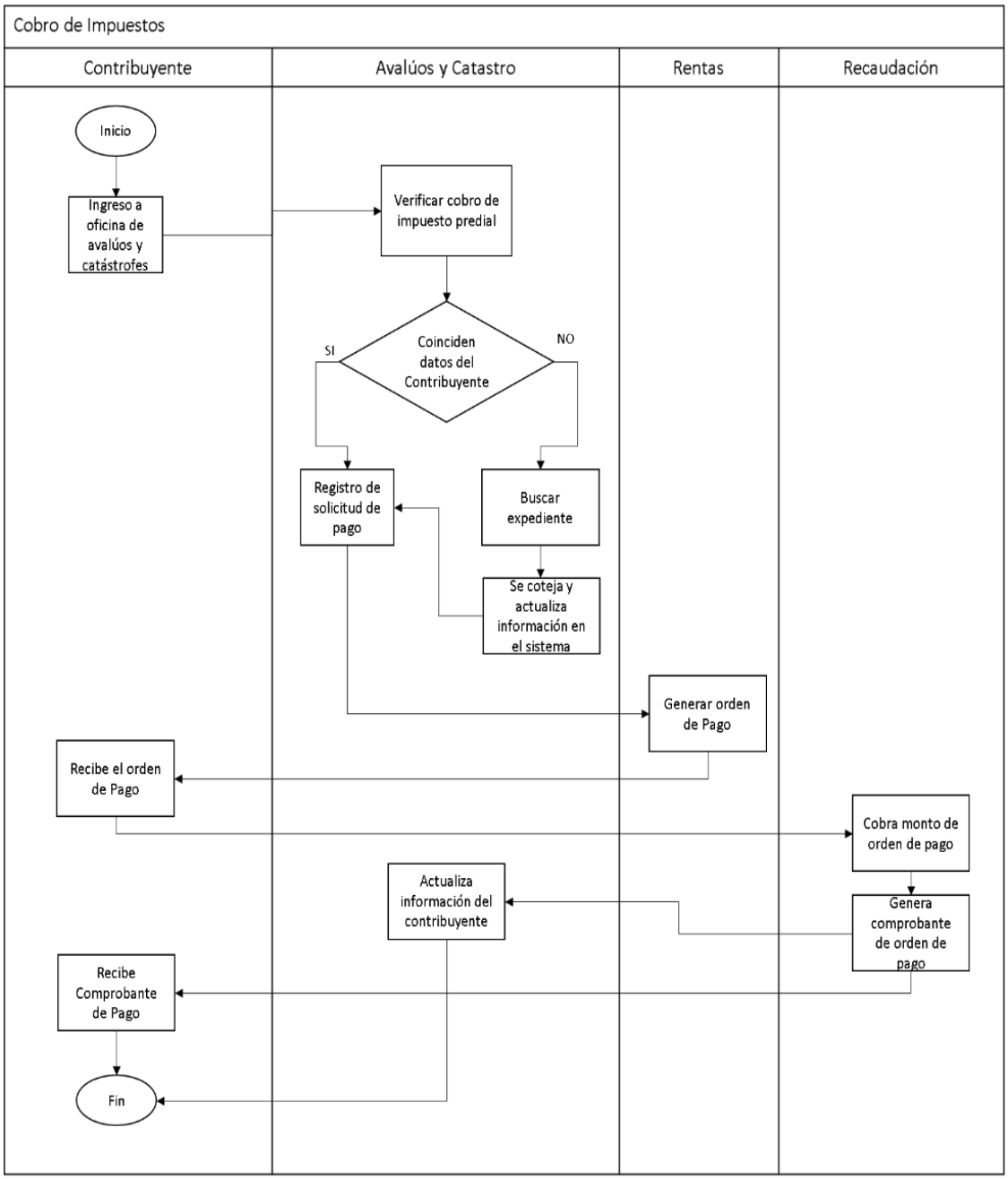


Fig. 4 Diagrama del cobro de impuestos

Fuente: Elaboración propia

Objetivo: Recaudar el respectivo pago de los impuestos a los contribuyentes evitando sanciones y multas.

Proceso 2: Extensión de permisos de funcionamiento

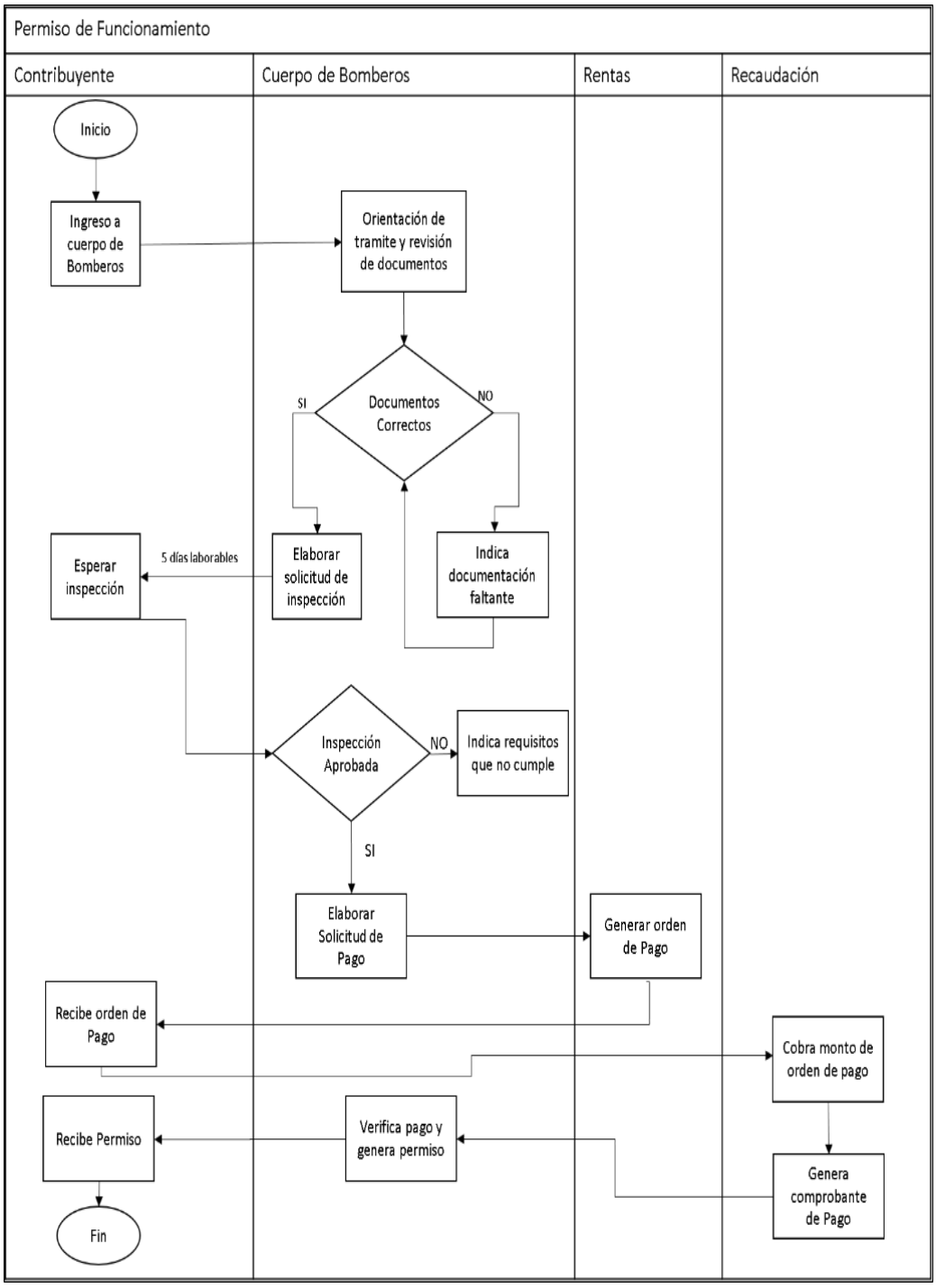


Fig. 5 Diagrama de permiso de funcionamiento

Fuente: Elaboración propia

Objetivo: Brindar permisos a los contribuyentes para negocios o locales comerciales, que deberán cumplir requisitos y realizar un respectivo pago.

Proceso 3: Extensión de permisos de suelo

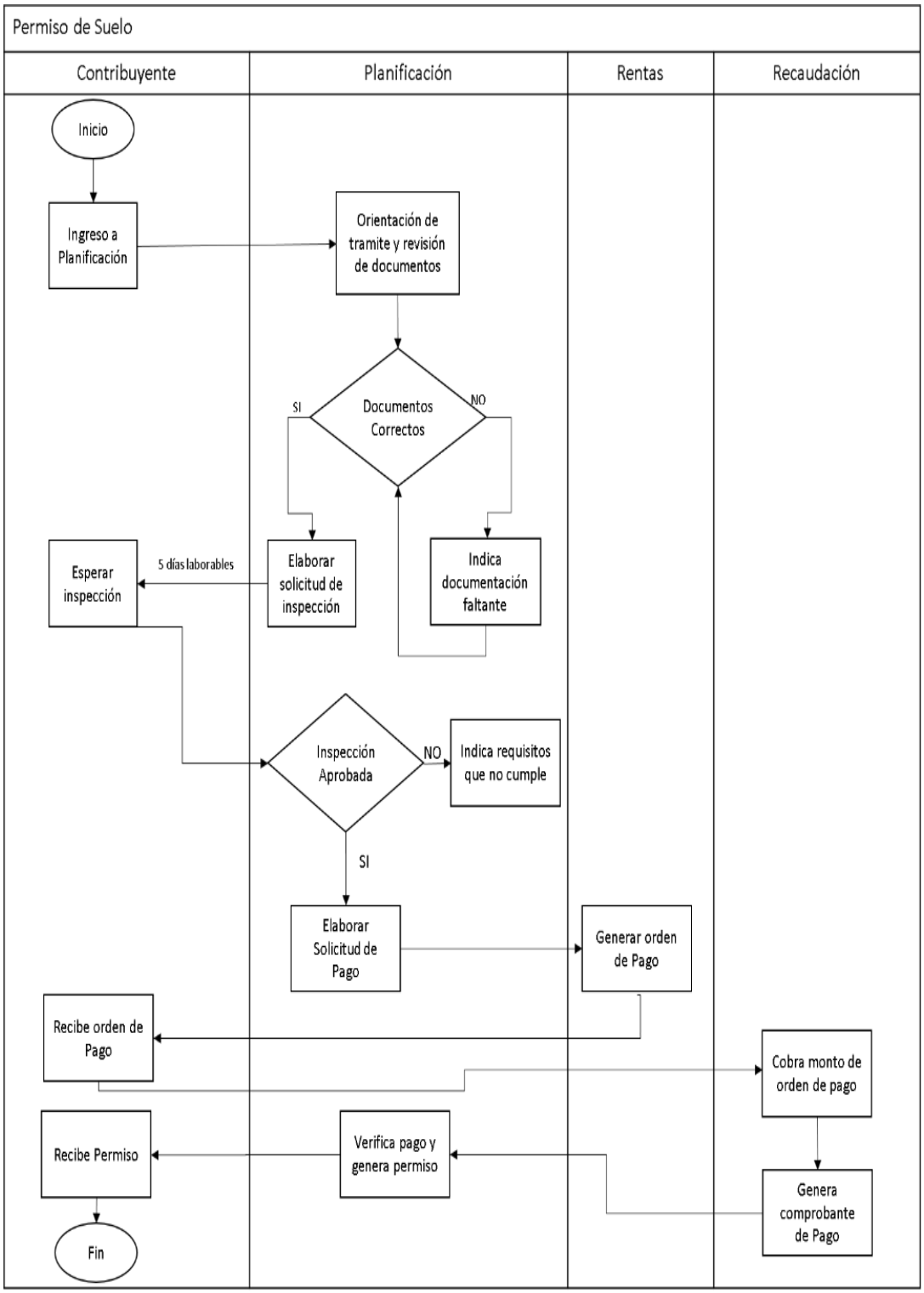


Fig. 6 Diagrama de permiso de suelo

Fuente: Elaboración propia

Objetivo: Permitir a los contribuyentes acceder a un permiso de suelo para la realización de construcciones, derrocamientos, excavación, desbanque y cerramientos.

Proceso 4: Cobro de Agua Potable

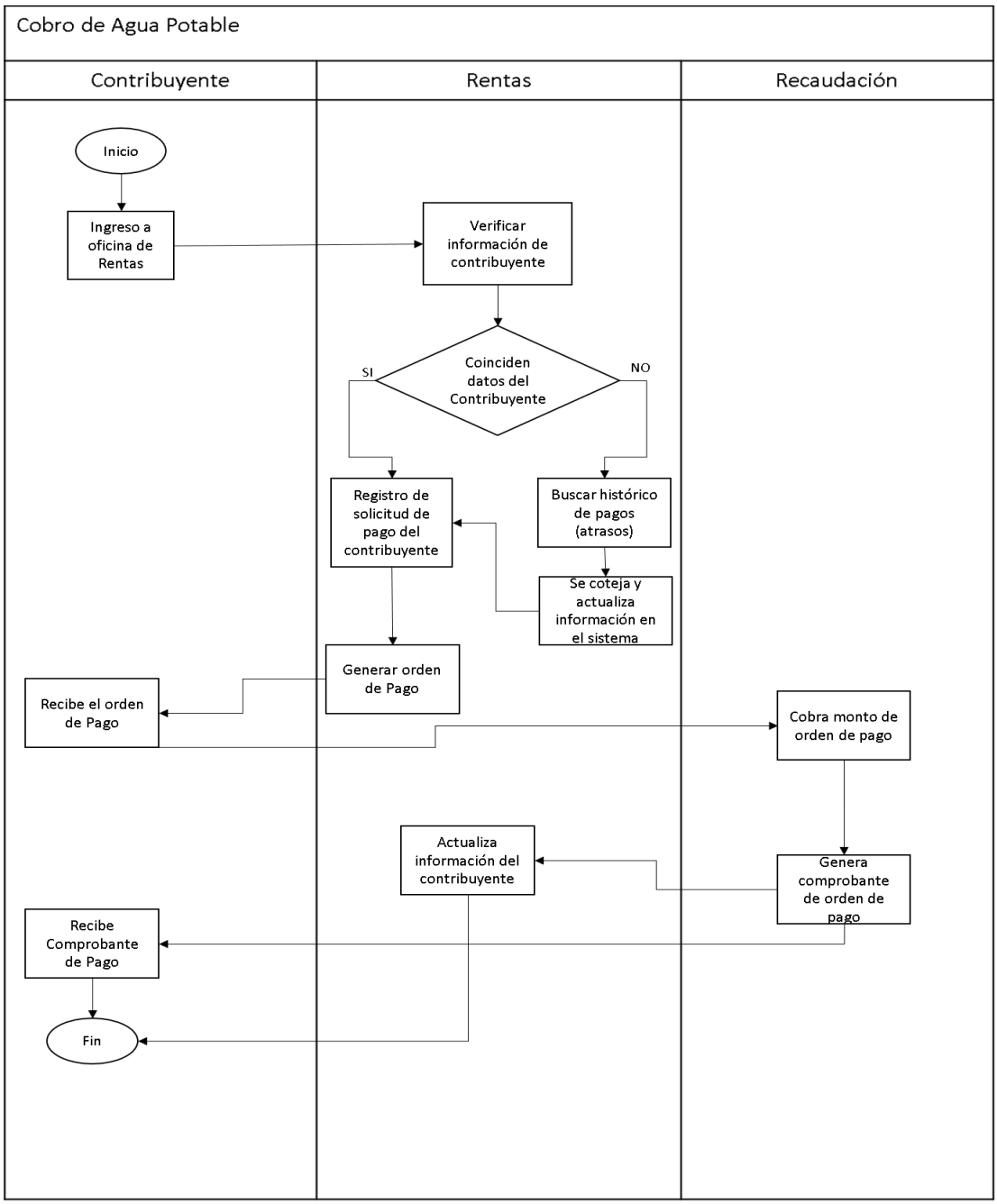


Fig. 7 Diagrama de cobro de agua potable

Fuente: Elaboración propia

Objetivo: Recaudar el pago del servicio básico de agua potable al contribuyente.

4.1.6 Análisis Informático Institucional

4.1.6.1 Estructura Organizacional del Área Informática

4.1.6.1.1 Organigrama Estructural vigente de Gestión Tecnológica

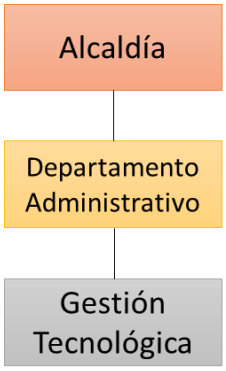


Fig. 8Organigrama Estructural vigente de Gestión Tecnológica
Fuente: Elaboración propia

4.1.6.1.2 Organigrama Funcional vigente de Gestión Tecnológica

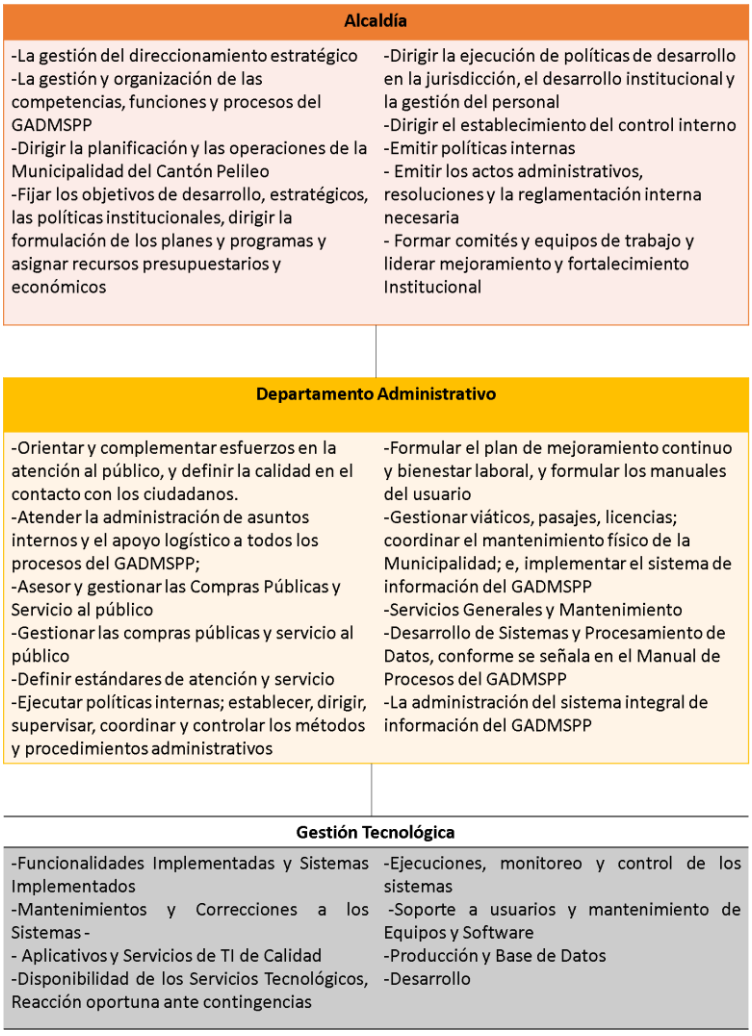


Fig. 9 Organigrama Funcional vigente de Gestión Tecnológica
Fuente: Elaboración propia

4.1.6.1.3 Organigrama Posicional de Gestión Tecnológica

Fig. 10 Organigrama Posicional de Gestión Tecnológica
Fuente: Elaboración propia

4.1.6.2 Talento Humano de Gestión Tecnológica

Nombre	**Cargo**	**Formación**
Carrasco Perrazo Luis Guillermo	Jefe del Departamento Tecnológico	Ingeniero en Sistemas e informática
Flores Mazón Julio Adalberto	Especialista en Redes	Ingeniero en Electrónica
Guato Guevara Miguel Ángel	Especialista en Desarrollo	Ingeniero en Sistemas y Computación

Tabla 7 Talento Humano de Gestión Tecnológica
Fuente: Elaboración propia

4.1.6.3 Recursos Informáticos Organizacionales

Los recursos informáticos Hardware y Software de GAD de San Pedro de Pelileo están distribuidos por Departamento que a su vez se dividen en áreas como se muestra en la Tabla 8.

Departamento	**Áreas**
Administración General	-Alcaldía -Archivo -Comunicación Institucional -Consejo Municipal -Secretaria General -Compras Publicas -Gestión Tecnológica -Talento Humano

Departamento	Áreas
Agua Potable y Alcantarillado	-Aguan Potable -Alcantarillado -Laboratorio
Asesoría Jurídica	-Asesoría Jurídica
Auditoria Interna	-Auditoria Interna
Avalúos y Catastros	- Avalúos y Catastro
Desarrollo de la Comunidad	-Biblioteca -Junta de Derechos -Cultura -Desarrollo de la Comunidad -Economía Popular y Solidaria -Psicología -Turismo -Trabajo Social
Financiero	- Activos -Coactivos -Contabilidad -Dirección Financiera -Presupuesto -Rentas -Tesorería -Ventanillas
Administración de Justicia	-Comisaria Municipal -Justicia
Obras Publicas	-Obras Publicas
Orden y Control	-Orden Y Control
Planificación	-Planificación
Registro de la Propiedad	-Registro de la Propiedad
Departamento Públicos	-Camal Municipal -Gestión de Riesgos -Mercado República de Argentina -Plazas y Mercados -Seguridad Ciudadana -Riesgos -Seguridad y Riesgos -Servicios Públicos -Complejo la Moya

Tabla 8 Clasificación por área de los Departamentos de GAD de San Pedro de Pelileo
Fuente: Elaboración propia

4.1.6.3.1 Hardware disponible en el GAD Municipal de San Pedro de Pelileo

Departamento Municipal / Hardware	Administración General	Departamento de Agua Potable y Alcantarillado	Asesoría Jurídica	Auditoria Interna	Avalúos y Catastros	Desarrollo de la Comunidad	Departamento Financiero	Administración de Justicia	Departamento de Obras Publicas	Departamento de Orden y Control	Departamento de Planificación	Registro de la Propiedad	Departamento Públicos
1.-Equipos Generales													
Computador Escritorio	18	6	3	2	12	17	17	5	9	6	13	7	21
Portátil	6	1	0	1	1	1	3	0	0	1	1	0	2
Router	1	0	0	0	0	1	0	0	0	0	0	1	2
Switch	2	1	0	0	2	1	0	0	0	0	1	1	1
Servidor	8	0	0	0	0	0	0	0	0	0	0	1	1
Subtotal	35	8	3	3	15	20	20	5	9	7	15	10	27
2.-Perfifericos Principales													
Monitor	18	6	3	2	12	17	17	5	0	6	13	7	21
Impresora	15	3	1	3	7	14	19	5	5	3	2	10	19
Teclado	18	6	3	2	12	17	17	5	9	6	13	7	21
Mouse	18	6	3	3	12	17	18	5	9	6	13	7	22
Disco Externo	4	0	0		0	1	1	0	0	0	0	1	1
Subtotal	73	21	10	10	43	66	72	20	23	21	41	32	84
3.-Otros Equipos													
Scanner	2	0	0	1	1	0	0	0	0	0	0	0	0
UPS	2	0	0	0	1	0	1	0	0	0	1	0	0
Central IP	0	0	0	0	0	1	0	0	0	0	0	0	0
Subtotal	4	0	0	1	2	1	1	0	0	0	1	0	0
Total	112	29	13	14	60	87	93	25	32	28	57	42	111
Total de Dispositivos	703												

Tabla 9 Hardware disponible en el GAD Municipal de San Pedro de Pelileo
Fuente: Elaboración propia

4.1.6.3.2 Red Interna y Externa de Comunicaciones existentes en el GAD Municipal de San Pedro de Pelileo

a. Diagrama Red Interna y Externa de Comunicaciones

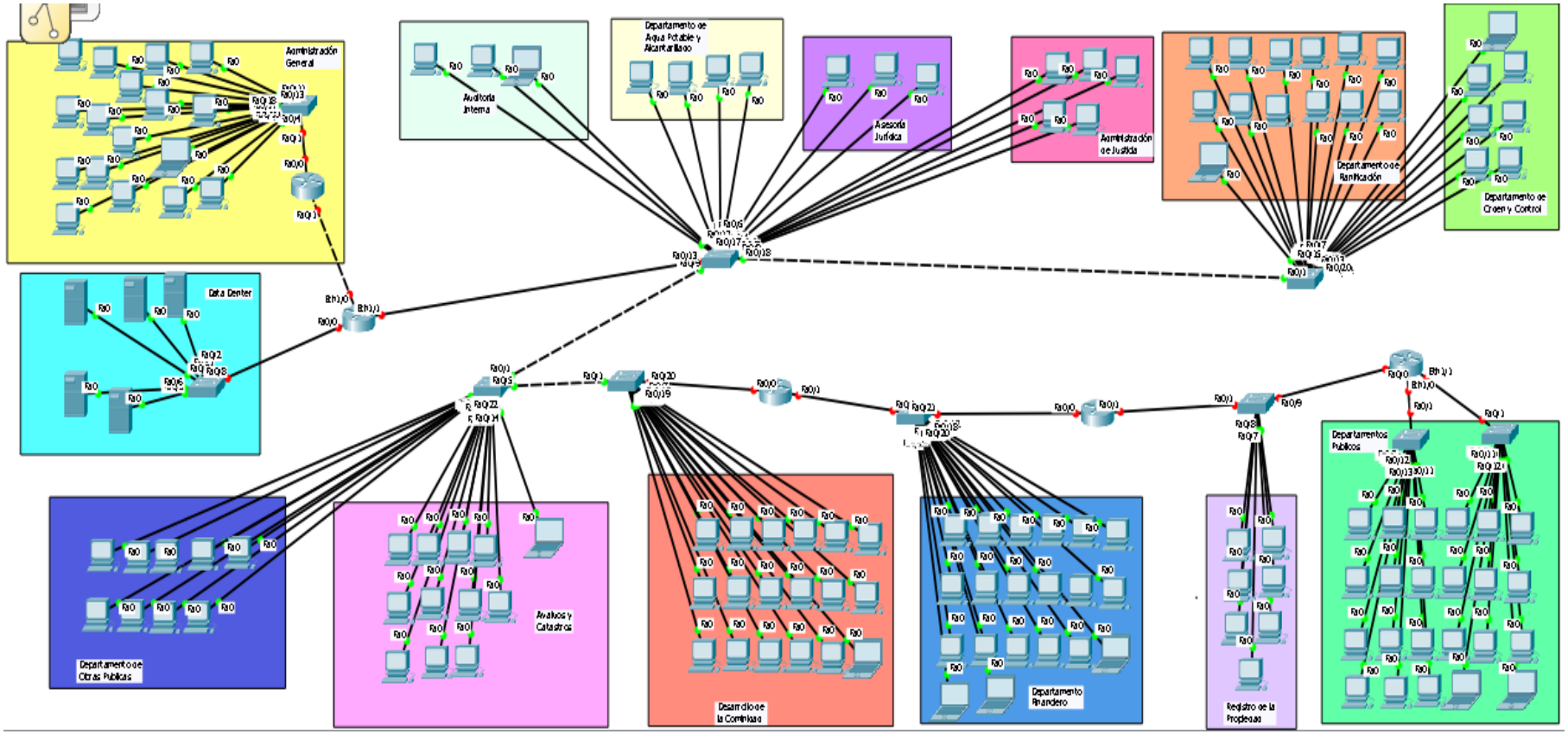


Fig. 11 Diagrama Red Interna y Externa de Comunicaciones
Fuente: Elaboración propia

b. Descripción General de los elementos de la red

Red Interna y Externa de Comunicaciones		
Componentes Principales	**Componentes Principales**	**Características Descriptivas**
CENTRAL IP GRANDSTREAM UCM 6202	-2 puertos FXS -2 puertos FXO Dos puertos de red Gigabit con PoE integrado -Registro detallado de llamadas (CDR) para monitorear el uso de teléfonos Soporta cualquier terminal de video SIP que emplee códecs H.264, H.263 o H.263+	La centralita Grandstream UCM6202 proporciona una solución a las necesidades de comunicación de la empresa. Combina funciones de voz, video, datos y movilidad en una misma solución muy fácil de utilizar; además, puede ser gestionada remotamente y ofrece tecnologías como voz, videollamada, videoconferencia, videovigilancia, entre otras.
SWITCH 54p capa3 CISCO SG300-52P	-Gigabit Ethernet (cobre), cantidad de puertos: 52 -Tecnología de cableado ethernet de cobre: 1000BASE-T, 100BASE-TX, 10BASE-F -Memoria interna: 128 MB -Tabla de direcciones -MAC: 16384 entradas	Es un portafolio de switches administrados asequibles que brinda una base confiable para su red empresarial. Estos switches proporcionan las funciones que necesita para mejorar la disponibilidad de sus aplicaciones empresariales críticas, proteger la información confidencial y optimizar el ancho de banda de la red para brindar información y aplicaciones con mayor eficacia
(X3) SWITCH 24p CISCO SG102 -24	-Puertos:22 x 10/100/1000 + 2 x combo SFP -24 puertos - no gestionado -Capacidad de conmutación: 48 Gbps -Rendimiento de reenvío (tamaño de paquete de 64 bytes): 35.7 Mpps	Ofrece alto rendimiento, fiabilidad y ahorro de energía diseñado para Empresas. Es muy fácil de usar sólo tiene que enchufar y listo no requiere ningún tipo de administración.

Red Interna y Externa de Comunicaciones		
Componentes Principales	**Componentes Principales**	**Características Descriptivas**
ROUTER MIKROTIK RB3011	-Procesador ARM dual core 1.4GHz, 1 GB de RAM -10 puertos 10/100/1000 Mbps -1 puerto SFP, 1 puerto USB 3.0, LCD. -Montaje en Rack Alimentación: DC Jack o PoE Pasivo	Primero en ejecutar una CPU de arquitectura ARM para un rendimiento superior. Permite agregar almacenamiento o un módem 3G / 4G externo. La unidad RB3011UiAS-RM viene con un gabinete de montaje en rack de 1U, un panel LCD de pantalla táctil, un puerto de consola serie y funcionalidad de salida PoE en el último puerto Ethernet.
(X3) SWITCH 24p HP g913a	- Switch Administrable Capa 2 vía Web y CLI - Dispone de 24 puertos RJ-45 Gigabit 10/100/1000 Mbps - Procesador MIPS a 500 MHz, SDRAM 128 MB y Flash 32 MB - Estándar IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.1q/p - Puertos MDIX automático, dúplex medio o completo - Capacidad de conmutación 48 Gbps - Capacidad de reenvío 35.7 Mpps - Tabla de Direcciones MAC 8k - Soporta hasta 4096 VLANs simultáneamente	El Switch Administrable Capa 2 Gigabit de 24 puertos de HP, ofrece alto rendimiento, fiabilidad, seguridad, QoS, creación de VLANs, enlaces troncales. Está diseñado para pequeña y mediana empresa SMB muy fácil de usar y administrar.
(X2) SWITCH 24p 3COM	- 24 puertos con autodetección y autoconfiguración - Velocidad total sin bloqueo en todos los puertos Ethernet, auto negociación y control de flujo bidireccional / semidúplex, establecimiento de prioridades de tráfico, 802.1p -Soporta hasta 4000 direcciones MAC	Es un switch sin bloqueo y sin necesidad de administración diseñado para oficinas pequeñas a medianas. Este switch de clase empresarial, que se puede instalar en un rack, puede colocarse en el armario de cableado o como unidad autónoma.

Red Interna y Externa de Comunicaciones		
Componentes Principales	**Componentes Principales**	**Características Descriptivas**
(X3) ROUTER MIKROTIK RB951UI-2HND	-Wi-Fi 2.4 GHz de gran cobertura Antena 2.5 dBi hasta 1 Watt de Potencia -Alimentación y Salida PoE (Pasivo) -Puerto USB para Memoria USB para uso de FTP	Es un dispositivo de red inalámbrico compacto que es perfecto para su pequeña oficina u oficina doméstica. No requiere mucho espacio premium. Sin embargo, a pesar de su tamaño, está cargado con muchas funciones pesadas que pueden dar a otros puntos de acceso.
SWITCH 24p TPLINK SG1024D	- 24 puertos a 10/100/ Mbps -Learning) y negociación MDI/MDIX automática - Diseño Plug & Play	Incluye Innovadora tecnología de eficiencia energética que ahorra hasta un 20% de energía Soporta aprendizaje de direcciones MAC.
Software de Administración de la Red	**Especificaciones Técnicas**	**Características descriptivas**
FIREWALL SOPHOS XG	-Instalación en entorno Virtual VMware, Citrix, Microsoft Hyper-V y KVM.	- Controla el estado de la red - Identifica los sistemas infectado -Aísla infecciones de forma automática -Controla Sincronizado de Aplicaciones

Tabla 10 Descripción General de los elementos de la red
Fuente: Elaboración propia

4.1.6.3.3 Software disponible en el GAD Municipal de San Pedro de Pelileo

Departamento Municipal	Software			
	Sistemas	**Gestión**	**Ingeniería o Científico**	**Computadoras Personales**
Administración General	-Windows Server 2003 R2 y 2008 R2 -Windows XP, Vista,7,8.1,10. -Centos 6.5	- ERPCabildo32 -Oracle 11g	-NetBeans IDE 7.2 - Pycharm IDE - AutoCAD 2015 Servipack 2 - ArcGIS 10	-Office 2007, 2010,2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Departamento de Agua Potable y Alcantarillado	-Windows 8.1	- ERPCabildo32	-	-Office 2007 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Asesoría Jurídica	Windows 10	-	-	-Office 2010 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Auditoria Interna	Windows 10	-	-	-Office 2007 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™

Departamento Municipal	Software			
	Sistemas	**Gestión**	**Ingeniería o Científico**	**Computadoras Personales**
Avalúos y Catastros	Windows 7, 8.1,10	- ERPCabildo32	-ArcGIS 10 -AutoCAD 2015 Servipack 2	-Office 2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Desarrollo de la Comunidad	Windows 8.1,10	-	-	-Office 2007, 2010,2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Departamento Financiero	Windows 8.1,10	- ERPCabildo32	-	-Office 2007, 2010,2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Administración de Justicia	Windows 8.1	-	-	-Office 2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™

Departamento Municipal	Software			
	Sistemas	**Gestión**	**Ingeniería o Científico**	**Computadoras Personales**
Departamento de Obras Publicas	Windows 7, 8.	- ERPCabildo32	-	-Office 2010 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Departamento de Orden y Control	Windows 10	- ERPCabildo32	-	-Office 2007, 2010 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Departamento de Planificación	Windows 7, 8.1,10	- ERPCabildo32	-	-Office 2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™

Departamento Municipal	Software			
	Sistemas	**Gestión**	**Ingeniería o Científico**	**Computadoras Personales**
Departamento Públicos	Windows 7, 8.1,10	-	-	-Office 2007, 2010,2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™
Registro de la Propiedad	Windows 8.1	- ERPCabildo32	-	-Office 2013 -Adobe Flash Player 31 -ESET NOD32 Antivirus -Google Chrome - Mozilla FireFox™

Tabla 11 Software disponible en el GAD Municipal de San Pedro de Pelileo
Fuente: Elaboración propia

4.1.6.4 Sistema de Información disponibles en el GAD Municipal de San Pedro de Pelileo

Sistemas de información	Descripción General	Software de Desarrollo	Usuarios	Procesos Cubiertos	Apoyo a Procesos y áreas usuarias	Funcionamiento en Red
ERP Cabildo	Sistema Integrado que maneja la mayoría de funciones municipales.	JAVA ORACLE	-Administración General -Departamento de Agua Potable y Alcantarillado -Avalúos y Catastros -Departamento Financiero -Departamento de Obras Publicas - Departamento de Orden y Control - Departamento de Planificación - Registro de la Propiedad	-Tesorería -Rentas -Compras -Planificación -Seguimiento de Tramites -Módulos Coactivos -Gestión Financiera -Gestión de Obras Publicas -Administración de Usuarios	Departamento Tecnológico	Servidor local para manejo de procesos internos del municipio, mediante arquitectura cliente- servidor, acceso mediante IP de la intranet institucional y con los usuarios y contraseñas asignadas por el Departamento Tecnológico.
WEB PAGE	Página web para conocimiento publico	HTML PHP	Personas en General	-Información Municipal y de transparencia -Diferentes consultas del contribuyente	Departamento Tecnológico	Alojado en un servidor de la entidad y acceso mediante una IP Publica.
Intranet	Página web para empleados del municipio	HTML PHP	Personal de Municipio	-Consultas -Uso de Correo Electrónico -Información municipal interna (comunicados, informes, resoluciones)	Departamento Tecnológico	Alojado en un servidor de la entidad y tienen acceso las personas conectadas a la red interna.

Tabla 12 Sistema de Información disponibles en el GAD Municipal de San Pedro de Pelileo
Fuente: Elaboración propia

4.1.6.5 Análisis general del Departamento Tecnológico y recursos informáticos organizacionales

Ámbito	Situación Actual
1. Legal	- La contratación del personal se lo realiza mediante concurso de merecimientos como ampara la ley para las entidades Públicas. - Los equipos adquiridos son solicitados por el departamento tecnológico bajo las normas institucionales. - Software utilizado en su gran mayoría cuenta con licencias pagadas; aquí radica un problema debido a que infringe la ley al utilizar software sin licencia.
2. Departamento tecnológico	Los integrantes del Departamento Tecnológico son personas capacitas y preparadas en el ámbito informático y electrónico por lo que cumplen con las actividades asignadas.
3. Talento Humano	- Se rige bajo las disposiciones internas de la institución y están en constante comunicación para mejorar la relación interna del Departamento Tecnológico.
4. Hardware disponible	El Hardware que dispone cumple con las características necesarias para ejecutar las tareas que se necesitan en cada puesto de trabajo. Faltan dispositivos UPS para que se salvaguarde los dispositivos en caso de un corte de energía. En el caso de un daño de hardware el Departamento Tecnológico se encarga de su revisión y realizara la reparación o en caso de no tener solución dar de baja para la posterior reposición. Los dispositivos de impresión tienen un mantenimiento realizado por empresas de terceros.
5. Red Interna y Externa de Comunicaciones existente	- Cuenta con una red de fibra óptica, revisada y certificada por estándares internacionales. - La red de comunicación interna y externa brinda buena conectividad para poder cumplir con las tareas necesarias.
6. Software disponible	- El software que la empresa dispone es el adecuado para las actividades cotidianas del Municipio. - El software está bajo las debidas licencias pagadas de las empresas que lo distribuyen, además se utiliza software de libre distribución y versiones de prueba.

Ámbito	Situación Actual
7. Sistemas de Información disponible	- En el sistema integrado se realiza la mayoría de actividades de la institución. - Dispone de una página web que sirve de información y consulta para los contribuyentes y otra exclusiva para los miembros de la entidad.

Tabla 13 Análisis general del Departamento Tecnológico y recursos informáticos organizacionales
Fuente: Elaboración propia

4.1.7 Interpretación de Resultados del Análisis de TI.

4.1.7.1 Resultados de la Encuesta

La encuesta se realizó a un total de 32 empleados del GAD Municipal de Pelileo que son quienes intervienen directamente en los procesos de recaudaciones y permisos utilizando los medios de TI que el departamento tecnológico provee.

Los resultados de la encuesta realizada al personal del GAD Municipal de San Pedro de Pelileo, se muestran a continuación:

1. ¿La seguridad de la información manejada en la institución es adecuada?

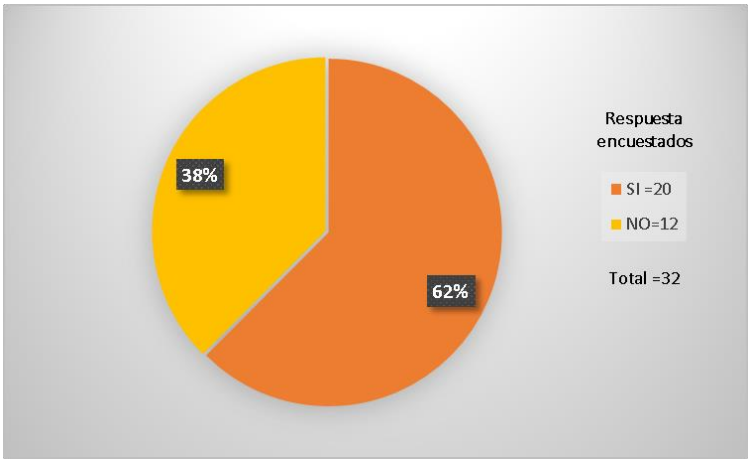


Fig. 12 Seguridad de la Información

Fuente: Elaboración propia

Análisis e Interpretación: Del total de encuestados el 62% considera que la seguridad de la información que maneja la entidad pública es adecuada, mientras que el 38% indica lo contrario, es decir que la seguridad de la información no es totalmente adecuada en la institución.

2. ¿La información es restringida a personas ajenas a la institución?

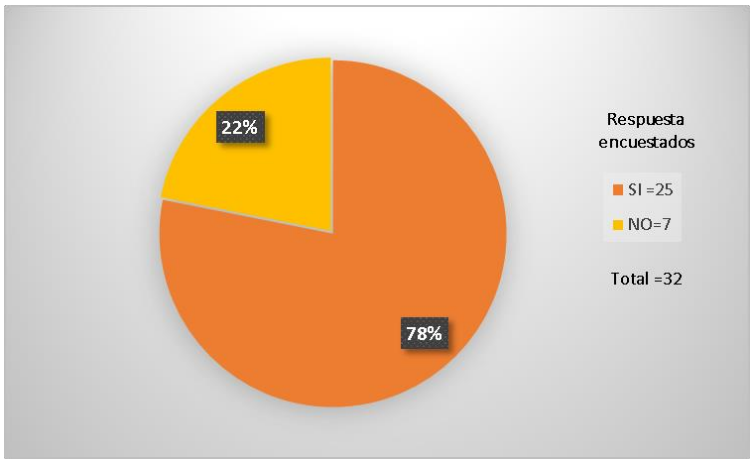


Fig. 13 Acceso a la Información

Fuente: Elaboración propia

Análisis e Interpretación: La mayoría de encuestados indica que la información tiene acceso restringido para personas ajenas a la institución mientras que una minoria indica lo contrario, es decir, que la información se encuentra disponible al público en general en ciertas áreas del Municipio.

3. ¿Considerar que se debe mejorar el manejo de la información y los equipos informáticos en el GAD de San Pedro de Pelileo?

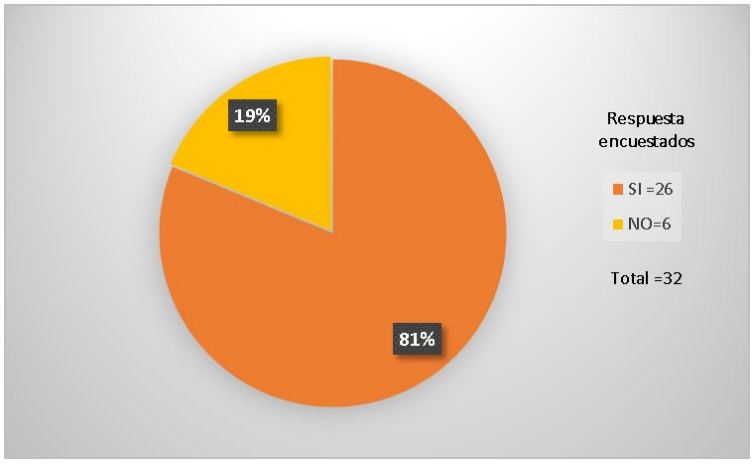


Fig. 14 Manejo de la Información

Fuente: Elaboración propia

Análisis e Interpretación: Casi la totalidad de encuestados coincide que se debe mejorar el manejo de la información y los quipos informáticos en el GAD de San Pedro de Pelileo; es decir, el manejo de la información y equipos no es la adecuada en la institución.

4. ¿Se realizan copias de seguridad de la información en la institución?

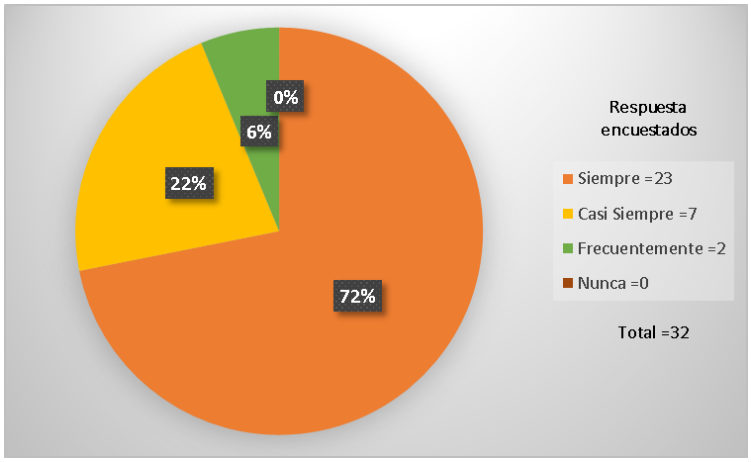


Fig. 15 Frecuencia de respaldos

Fuente: Elaboración propia

Análisis e Interpretación: Del 100% de encuestados, el 72% siempre realiza copias de seguridad de la información, el 22% casi siempre realiza copias de seguridad de la información, el 6% realiza frecuentemente copias de seguridad, y finalmente un 0% opino que nunca realiza copias de seguridad, la información está respaldada satisfactoriamente.

5. ¿Se establecen claves exclusivas para su área de trabajo?

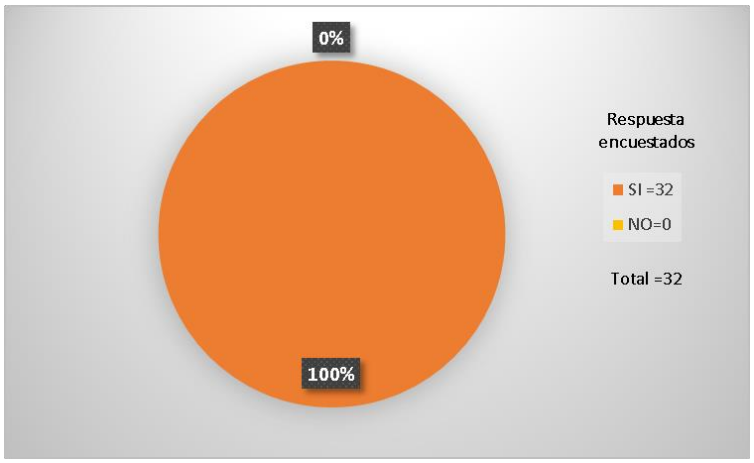


Fig. 16 Claves exclusivas

Fuente: Elaboración propia

Análisis e Interpretación: La totalidad de encuestados tienen claves exclusivas para su área de trabajo que son administradas por el jefe del Departamento Tecnológico para tener mayor seguridad de la información.

6. ¿Tiene registradas sus claves en lugares visibles a otros usuarios (Notas, archivos)?

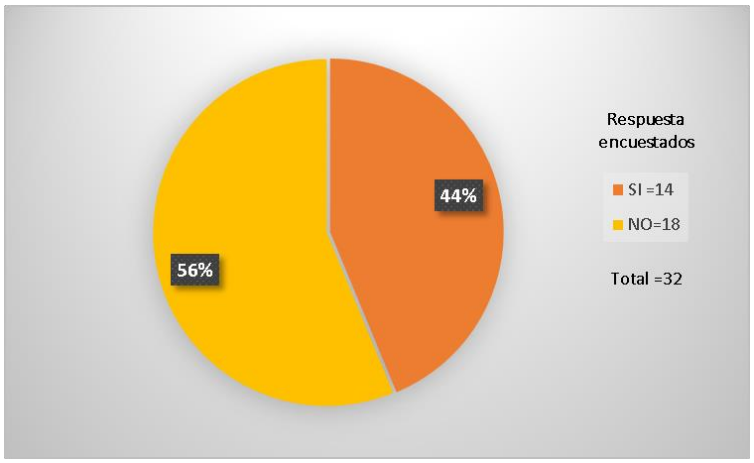


Fig. 17Claves expuestas

Fuente: Elaboración propia

Análisis e Interpretación: De un total de 32 encuestados, el 56% no tiene sus claves registradas en lugares visibles, mientras que 44% tiene sus claves personales registradas en archivos visibles de fácil acceso, permitiendo el acceso a terceros y a más personas ajenas a la institución a dichas claves.

7. ¿Con que frecuencia se cambian sus claves de acceso en su puesto de trabajo?

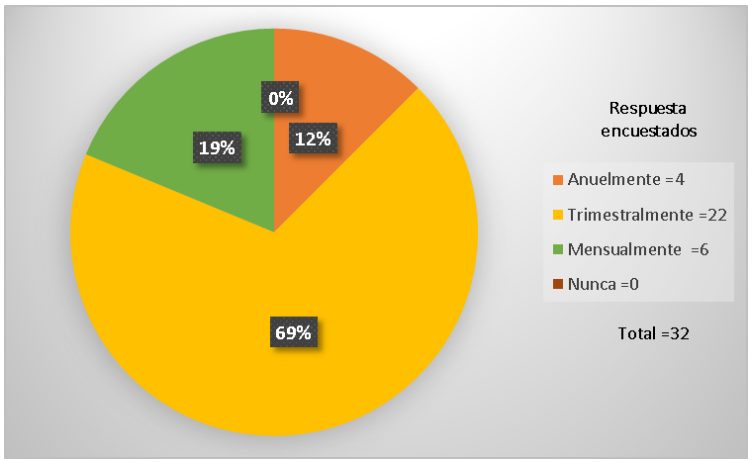


Fig. 18 Frecuencia de cambio de clave

Fuente: Elaboración propia

Análisis e Interpretación: Del 100% de encuestados el 69% cambia sus claves de acceso Trimestralmente, el 19% cambia sus claves de acceso mensualmente y un 13% lo realiza anualmente, el administrador es el encargado de proporcionar las claves.

8. ¿Han realizado auditorías Informáticas en su área de trabajo?

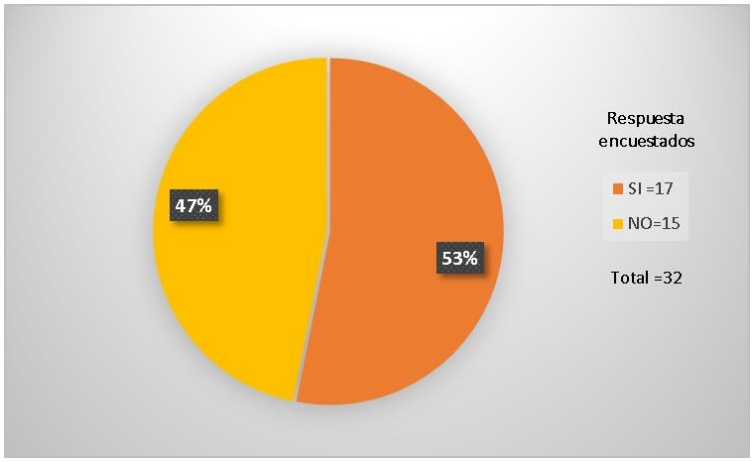


Fig. 19 Auditoria Informática en áreas de trabajo

Fuente: Elaboración propia

Análisis e Interpretación: De un total de 32 encuestados, el 53% ha realizado auditorias informáticas en su área de trabajo y un 47% no si ha realizado alguna auditoria informática en su área de trabajo, por consiguiente, no se han detectado malos funcionamientos de sistemas y malas prácticas de seguridad.

9. ¿Cree que el sistema informático que utiliza es adecuado para sus funciones?

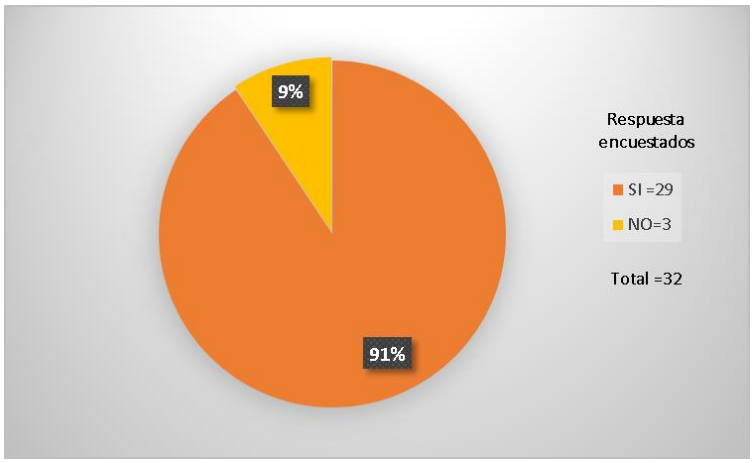


Fig. 20 Sistema adecuado

Fuente: Elaboración propia

Análisis e Interpretación: De un total de 32 encuestados el 91% indica que el sistema informático que maneja si es el adecuado para las funciones que realizan mientras que un 9% indica que el sistema informático no cumple con todas las funciones que necesitan en su lugar de trabajo por lo cual no son adecuados para cumplir con sus funciones diarias.

10. ¿Con que frecuencia el sistema informático presenta fallas?

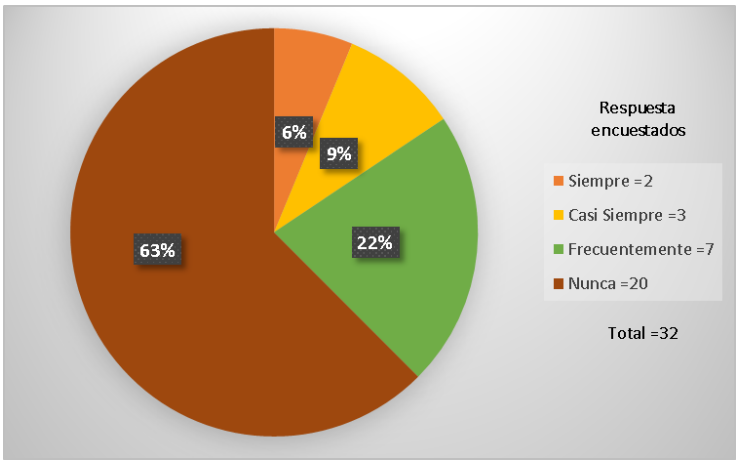


Fig. 21 Frecuencia de fallas en los sistemas informáticos

Fuente: Elaboración propia

Análisis e Interpretación: De un total de 32 encuestados el 63% indica que el sistema informático no presenta fallas, el 22% indica que esto sucede frecuentemente, el 9% indica que casi siempre se presentan fallas y finalmente un 6% que indica que siempre existen fallas en el sistema informático, lo que causa que en algunas áreas el trabajo se desarrolle de forma ineficiente.

4.1.7.2 Resultados de la entrevista

La entrevista se realizó al jefe del Departamento Tecnológico, el cual indico lo siguiente:

ENTREVISTA REALIZADA AL JEFE DEL DEPARTAMENTO TECNOLOGICO DEL GAD DE SAN PEDRO DE PELILEO			
Objetivo:	Recolectar información del manejo de la seguridad de la información en el GAD de San Pedro de Pelileo.		
Fecha:	10/10/2018		
Entrevistado:	Ing. Luis Carrasco	**Entrevistador:**	Oscar Silva
Cargo:	Jefe del Departamento Tecnológico		

N.º	**Preguntas**	**Respuestas**
1	¿El personal con el que cuenta el área de informática es el adecuado para cumplir las funciones designadas?	El personal con que se dispone si es el adecuado debido a que son profesionales preparados en el área informática.

ENTREVISTA REALIZADA AL JEFE DEL DEPARTAMENTO TECNOLOGICO DEL GAD DE SAN PEDRO DE PELILEO		
2	¿El personal del área está capacitado para realizar las tareas que desempeñan?	Cada miembro del área informática tiene sus funciones bien definidas y para las que se realiza capacitaciones continuas.
3	¿Se requiere de servicios de terceros para cumplir con las funciones del área?	Si es necesario la intervención de terceros para que todo funcione correctamente, específicamente en lo se refiere a la reparación de hardware.
4	¿El área de informática cuenta con documentación donde establezca sus funciones?	Si se dispone documentación que organiza las responsabilidades y funciones de los integrantes del área informática
5	¿Cree usted que el presupuesto asignado por el GAD Municipal al área informática es el adecuado?	El departamento de sistemas siempre realiza solicitudes para que se asigne una mayor cantidad de presupuesto, pero lastimosamente los pedidos nos son atendidos.
6	¿Cree que el espacio físico del departamento tecnológico es el adecuado?	El espacio físico que el municipio asigno es un poco reducido, pero, hay que acoplarse a lo que se dispone. El espacio se nos hace pequeño por el aspecto servidores y lo relacionado al manejo de la red de la institución.
7	¿En caso de no encontrarse Ud. quién asume sus funciones?	En el caso de ausentarme quien toma mis funciones es el encargado de la administración de Redes Ing. Julio Flores

ENTREVISTA REALIZADA AL JEFE DEL DEPARTAMENTO TECNOLOGICO DEL GAD DE SAN PEDRO DE PELILEO		
8	¿Existen algún plan para la seguridad de la información de la institución?	En la institución si se cuenta con distintos planes de seguridad tanto preventivo como correctivo, siempre teniendo en cuenta que la información que se posee es de gran utilidad.
9	¿Con cuántos sistemas cuenta la institución y cual son sus funciones?	Se dispone de un solo sistema integrado llamado ERP Cabildo que prácticamente administra todo el GAD municipal.
10	¿Tiene programado realizar mantenimientos a los equipos informáticos? ¿Con que frecuencia los realiza?	Si se tienen mantenimientos principalmente en lo que a servidores se refiere se lo realiza, se tiene planificado realizar cada 3 meses, pero en ocasiones por motivos institucionales no se los realiza a tiempo, pero no se han presentado fallas mayores. En cuanto a otros equipos de oficinas se los realiza cuando el usuario del equipo lo requiera.
11	¿Cree que se da el mantenimiento adecuado a los equipos?	El mantenimiento de equipo a mi parecer es el adecuado, ya que la mayoría de veces es revisión del estado de software, en cuanto a hardware se refiere se utiliza terceros para reparaciones.

Tabla 14 Entrevista Jefe de Departamento tecnológico

Fuente: Elaboración propia

Después de haber realizado un análisis e interpretación de la información obtenida mediante encuestas, observación y entrevistas al personal del GAD Municipal de San Pedro de Pelileo, se obtuvo las siguientes conclusiones:

- La información que se manipula en el GAD Municipal de San Pedro de Pelileo, en su mayor parte correcta, pero hay ciertos sectores en los cuales dicha información no es protegida eficientemente ya personas ajenas a la institución podrían tener acceso a dicha información.
- Las claves son de uso único y asignadas por el departamento tecnológico para cada área de trabajo, pero por descuido o irresponsabilidad de ciertos empleados, pueden caer en manos de otras personas, por lo que podrían tener acceso a información que no les compete.
- La infraestructura no es la apropiada debido a que las instalaciones son muy pequeñas, además los servidores no cuentan con la seguridad adecuada.
- En la mayor parte de la institución realiza periódicamente copias de seguridad que permiten tener un respaldo y evitar perdida de información, pero hay ciertos sectores que no realiza esta acción habitualmente por lo que pone en riesgo esta información.
- El personal del área de informática de GAD Municipal de Pelileo es el adecuado en las áreas en las que se desempeñan, además cada uno tiene sus funciones bien definidas.
- El personal tiene programado mantenimiento de los equipos informáticos en su gran mayoría en el apartado de software, pero se necesitaría personal que se encargue del aspecto hardware.

Con todos estos antecedentes, información y conclusiones se da fiel cumplimiento a lo estipulado en el primer objetivo específico de esta investigación.

4.2 Alcance de la Auditoría Informática

En la auditoria a realizar el alcance está determinado por el marco referencial de la Metodología Octave, con el fin de mejorar el uso de las Tecnologías de Información para ello se realizará una evaluación de la posibles amenazas y vulnerabilidades operacionales que se pueda encontrar en los procesos de recaudaciones y permisos de la institución.

La recolección y valoración de información es la actividad inicial a desarrollar en la auditoria, permitirá evaluar si los procesos, los sistemas informáticos de la entidad y los activos de información que intervienen en dichos procesos, se utilizan correctamente y tienen un manejo adecuado de información.

Para este proyecto los procesos a revisar son aquellos que los miembros de la institución consideran que pueden tener mayor vulnerabilidad, al obtener la información de la institución y una vez identificado las áreas de preocupación, escenarios de amenaza y los posibles riesgos se procederá a realizar el análisis con el fin de generar opciones de mitigación o reducción de impacto de los distintos riesgos y amenazas encontradas. Las recomendaciones se las presentaran al jefe del Área Tecnológica quien decidirá si se aplica las medidas planteadas.

4.3 Recursos necesarios para la realización de la Auditoría.

Los recursos utilizados para la realización de la auditoria se encuentra las encuestas realizadas al personal que utilice sistemas informáticos en el GAD de San Pedro de Pelileo, además de una entrevista al jefe del Departamento Informático.

Por otro lado, la observación fue una parte principal del proyecto ya que por medio de ella se pudo evidenciar las actividades que se realiza en la institución y con esto verificar como se maneja la información.

Se requirió otros recursos que son:

Recursos materiales

Estos recursos materiales fueron brindados por la institución, debido a que se realizó un convenio para poder utilizar los activos de la institución tales como máquinas, uso de discos duros e impresoras.

Recursos humanos

Los recursos humanos tomados en cuenta es el personal del GAD municipal de San Pedro de Pelileo, al cual se le realizo las encuestas propuestas para esta auditoría y al jefe del área de tecnológica a quienes se les realizo la entrevista. El auditor en este caso mi persona Oscar Silva y el tutor del presente trabajo.

4.4 Elaboración del Plan de Auditoría

La metodología Octave, no da sugerencia de controles durante el desarrollo de su metodología, por tanto, se tomaron los dominios de la norma ISO 27001, que permiten

gestionar la seguridad de la información en los diferentes procesos de la entidad; estos dominios se incorporan en los activos que se van a proteger, con el fin de garantizar el correcto uso, operatividad y gestión de la información, dentro de los marcos legales.
Los dominios permiten identificar los riesgos, analizarlos y gestionar un plan de acción que permitan mitigarlos, teniendo en cuenta la integridad, disponibilidad y confidencialidad de la información.
Para el análisis del caso estudio se seleccionaron los dominios de la norma ISO 27001 que se muestran en la Tabla 14:

Dominios de Norma ISO 27001	
N.º	**Descripción**
Dominio 5	Políticas de seguridad de la Información.
Dominio 6	Organización de la seguridad de la información
Dominio 7	Seguridad de los Recursos Humanos
Dominio 8	Gestión de recursos.
Dominio 9	Gestión de acceso de usuario.
Dominio 11	Seguridad física y ambiental.
Dominio 12	Seguridad Operacional.
Dominio 13	Seguridad de las Comunicaciones.
Dominio 15	Relaciones con los proveedores.
Dominio 16	Gestión de Incidentes de Seguridad de la Información.
Dominio 17	Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio.
Dominio 18	Cumplimiento

Tabla 15 Dominios de la Norma ISO 270001

Fuente: Elaboración propia a partir de [35].

4.5 Identificación del nivel de conocimiento de los miembros de la entidad

4.5.1 Análisis de Dominios en el GAD Municipal de San Pedro de Pelileo

Cada dominio fue seleccionado conjuntamente con el analista de riesgos de la institución con el fin de evaluar la situación actual del Municipio de Pelileo en cuanto a seguridad de la información y la seguridad física de la misma.

En la Tabla 5 se muestra un análisis de cada uno de los objetivos de control en relacionado con la Institución.

Análisis de Dominios		
N.º	**Dominio**	**Análisis**
Dominio 5	Políticas de seguridad de la Información.	Las políticas de seguridad son analizadas por la junta directiva y comisiones de recursos humanos en la cual indican claramente las necesidades que tiene la organización, en cuanto a la seguridad de la información, teniendo en cuenta algunos riesgos presentados anteriormente en la municipio, estas políticas van dirigidas a todo el personal de la entidad, una vez elaboradas las políticas deben ser revisados y aprobadas por la junta directiva, a su vez los empleados son informados sobre las mismas y además se publica en la página web de la organización.
Dominio 6	Organización de la seguridad de la información	El municipio no cuenta con una persona o un área que se encargue directamente de la seguridad de la información, en el área de sistemas existen 3 personas, el jefe del departamento, encargado de redes y encargado de desarrollo que tienen establecidas sus funciones, pero con nula la presencia de políticas de seguridad de la información, por lo que es posible que la información de la institución sea vulnerable; hoy en día la entidad cuenta con varios sistemas incluido la plataforma de recaudo, que es de mucha importancia en el aspecto financiero de la institución.

Análisis de Dominios		
N.º	**Dominio**	**Análisis**
Dominio 7	Seguridad de los Recursos Humanos	El Municipio de Pelileo para la contratación de personal realiza un concurso de merecimientos, posteriormente al personal contratado se solicita variedad de documentación con datos personales que serán guardados en el sistema, además se solicita al jefe del departamento se cree un nuevo usuario en el directorio activo. Cuando ingresa el nuevo personal ya tiene tareas predefinidas, se le proporciona los medios y la información necesaria para que pueda cumplir las actividades correspondientes a su cargo, además se realiza capacitaciones de las herramientas tecnológicas que usa la entidad. En caso de que se implemente una nueva tecnología se realiza una capacitación general explicando cada una de las amenazas informáticas o fraudes que se pueden encontrar por medio del correo electrónico.
Dominio 8	Gestión de recursos.	Las características que se deben registrar en el inventario son clasificación, valoración, ubicación y acceso de la información. Existen una gran variedad de activos de información tales como las bases de datos, documentación del sistema, manuales de usuario, procedimientos operativos, registros de auditoría, registros de licencia, activos de software, activos físicos; todos los activos informáticos deben estar inventariados y esto está a cargo del departamento tecnológico del municipio.

		El uso de dispositivos de almacenamiento externo en los equipos de la institución solo se lo realiza con el consentimiento de la persona que esté a cargo del equipo de cómputo esto con el fin de evitar fuga de información, si algunos de los documentos que se necesitan están en servidores de almacenamiento (la nube) tales como Drive, Dropbox deben ser descargados por el área de sistemas con autorización del dueño del documento o a su vez el encargado.
Análisis de Dominios		
N.º	**Dominio**	**Análisis**
Dominio 11	Seguridad física y ambiental.	El Municipio cuenta con seguridad en cada uno de los ingresos a la institución principal, allí también se ubica unas varias cámaras alrededor de la propiedad, en el parqueadero se encuentra una puerta que se abre manualmente, este acceso es solo para guardar los vehículos. El Data Center no tiene seguridades para el acceso ya que para ingresar solo existe una puerta corrediza, además en el departamento tecnológico no se encuentra ningún tipo de vigilancia por lo que es una zona vulnerable. Cuentan con planes de contingencia en caso de terremotos, explosiones, pero no son aplicados, tampoco se realizan simulaciones contra desastres naturales, en caso de corte de energía no cuenta con una planta, en caso de incendio no se cuenta con detectores de humo, solo en ciertos departamentos cuenta con un extintor.

Análisis de Dominios		
N.º	**Dominio**	**Análisis**
Dominio 12	Seguridad Operacional.	El área de sistemas de la Municipalidad de Pelileo se encarga entre otras cosas de asegurar que los equipos del personal cuenten con antivirus, actualmente cuenta con un proceso de Backup definido mediante un sistema de espejo (RAID), se sacan copias diarias de información y los Backup se almacenan en servidor ubicado en la casa del jefe de Departamento Tecnológico. Para la instalación de un nuevo producto o servicio en la institución, el área de sistemas primero realiza distintas pruebas para verificar un correcto funcionamiento.
Dominio 13	Seguridad de las Comunicaciones.	El municipio de Pelileo cuenta con un Data Center, no dispone un control de acceso presentado una falencia de seguridad, cuenta con una unidad de enfriamiento portátil para los servidores, tiene tan solo un UPS que no es suficiente en caso de que la entidad se quede sin energía, además se puede añadir que el espacio físico es reducido. También se encuentra la distribución de la red, para las diferentes áreas de la entidad, como son la alcaldía, administrativos, información, biblioteca municipal, recursos humanos, avalúos y catastros, contabilidad, departamento tecnológico, ventanillas de recaudación, entre otras.

Análisis de Dominios		
N.º	**Dominio**	**Análisis**
Dominio 15	Relaciones con los proveedores.	El Municipio maneja el contrato con los proveedores de manera legal, estableciendo compromisos y sanciones por incumplimiento, así mismo como fechas de las entregas, compromisos y responsabilidades adquiridas, estos contratos están supervisados por abogados contratados por prestación de servicio por la entidad.
Dominio 16	Gestión de Incidentes de Seguridad de la Información.	El Municipio de Pelileo, no cuenta con políticas de seguridad establecidas que indiquen cuál es el procedimiento a seguir en caso de presentarse un ataque a la seguridad de cualquier servidor o sistema, si llega a presentarse algún incidente de este tipo se responde de manera correctiva, más no se tiene un plan preventivo.
Dominio 17	Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio.	El Municipio de Pelileo cuenta con planes de contingencia para dar continuidad la entidad, pero, no se ha implementado, por ejemplo: pararrayos, detectores de humo entre otras. La institución no cuenta con un plan para restablecer la operación de la entidad luego de un desastre natural.
Dominio 18	Cumplimiento	El Municipio no cuenta con un área de auditoría, no obstante, se han realizado varias auditorias programadas que tratan de identificar las falencias y corregirlas. El Departamento Tecnológico, está realizando mejoras y monitoreos constantes con el fin de asegurar que la información este seguro, implementando nuevos procesos, proponiendo proyectos, capacitando al personal, realizando y mejorando los manuales de las aplicaciones

Tabla 16 Análisis de Dominios en el GAD Municipal de San Pedro de Pelileo
Fuente: Elaboración propia

4.5.2 Establecer criterios de medición del riesgo

Se establece los controles organizacionales que serán utilizados para la evaluación, estos son tomados de acuerdo al grado de impacto que afecte a la visión y misión de la organización.

El GAD municipal de San Pedro de Pelileo tiene su objetivo definido, pero como en este proyecto se enfoca en los procesos de recaudación y permisos se tomaron en cuenta los siguientes criterios.

- Reputación
- Financiera
- Productividad
- Seguridad/salud
- Legal [36]

Para el desarrollo de este paso se establecieron criterios a partir de la siguiente tabla:

Área de impacto	**Criterio de medición de riesgo**		
	Bajo	**Moderado**	**Alto**
Financiera	Reclamos esporádicos por parte del contribuyente.	Incremento de reclamos por parte de los contribuyentes hasta en un 50% de un semestre a otro	Incremento de reclamos por parte de los contribuyentes hasta en más de un 50% de un semestre a otro
Productividad	Interrupción de las operaciones municipales por menos de 4 horas laborables	Interrupción de las operaciones municipales entre 4y 12 horas laborables	Interrupción de las operaciones municipales entre 13 y 24 horas laborables. No hay atención a los contribuyentes
Reputación	Comentarios injuriosos o malintencionados	Campaña de desprestigio	Impacto que afecte la imagen de la institución pública frente al pueblo.

Área de impacto	Criterio de medición de riesgo		
	Bajo	**Moderado**	**Alto**
Legal	No genere sanciones o pérdidas económicas de la institución.	Llamado de atención por parte de entes de control	Sanciones económicas a la institución por parte de autoridades legales o entes reguladores
Seguridad /Salud	incapacidad menor a 3 días	incapacidad entre 3 y 100 días	incapacidad entre 100 y 365 días

Tabla 17Criterios de medición de riesgo

Fuente: Elaboración propia a partir de [37]

Una vez que se definió las áreas de impacto que se relacionan con las recaudaciones y permisos se procede a analizar y asignar un valor de importancia de acuerdo a la prioridad, es decir el área de impacto de más importancia tendrá un mayor valor (5) y así se irán reduciendo hasta legar al área de impacto de menor importancia (1), esto se realizara de acuerdo al criterio del auditor conjuntamente con los miembros área auditar.

Área de impacto	Prioridad
Financiera	5
Productividad	4
Legal	3
Reputación	2
Seguridad /Salud	1

Tabla 18 Asignación de prioridad de áreas de impacto

Fuente: Elaboración propia

4.6 Desarrollar un Perfil de los Activos Informáticos:

Los activos de los que se realiza un perfil son de aquellos que tiene valor para la organización en este caso se realizó el perfil de los activos de información que interfieren en los procesos ya mencionados anteriormente.

El perfil consiste en una descripción del activo en el que se detalla para que sirve, los medios de seguridad que este debe tener, el responsable del activo.

Para el desarrollo del activo se desarrolla 6 actividades que se detallan a continuación.

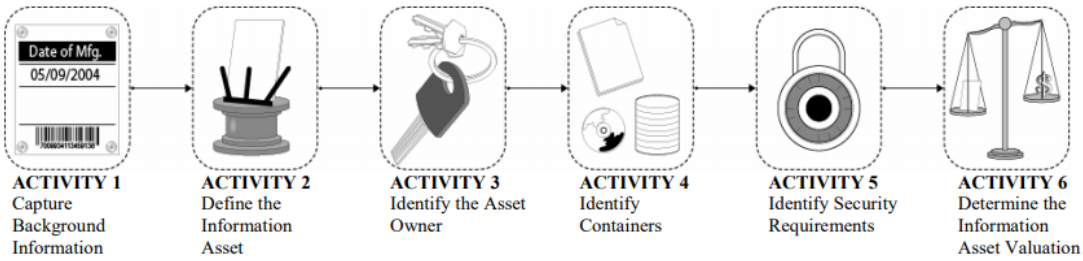


Fig. 22 Perfilamiento de activos

Fuente: [38]

Actividad 1- Capturar información de fondo:

El propósito de este paso es recopilar información, sobre la persona que está completando el perfil de activos de información, es probable que los activos de información evolucionen con el tiempo, por lo tanto, un perfil de activos de información puede necesitar ser actualizado o recreado. [38]

Actividad 2 -Definir el activo de información

El propósito de este paso es caracterizar un activo de información. Antes de que cualquier tipo de actividad de análisis pueda realizarse en un activo de información, la organización debe entender y acordar lo que contiene un bien de información.

El nivel de detalle que se captura debe ayudar en

• Definir el contenido de un activo y sus límites.

• Determinar la propiedad del activo

• Determinación de los requisitos de seguridad del activo [38].

Actividad 3 - Identificar al propietario del activo

El propósito de esta actividad es identificar y documentar el propietario del activo de información es importante porque el propietario debe trabajar con el individuo o grupo.

La propiedad de los activos de información a menudo es confusa para una organización. La identificación de la propiedad es una de las actividades más importantes para la seguridad efectiva y la gestión de riesgos de los activos de información que una organización puede realizar. Muchas organizaciones nunca han realizado un inventario preciso y completo de sus activos de información [38].

Actividad 4 - Identificar Contenedores

El propósito de este paso es capturar una lista de todos los contenedores en los que el activo se almacena, transporta o procesa y la lista asociada de los gestores de dichos contenedores.

En una evaluación de riesgos de seguridad de la información, la identificación de contenedores clave es esencial para identificar los riesgos para el activo de información en sí [38].

Actividad 5 - Identificar los requisitos de seguridad

El propósito de este paso es capturar los requisitos específicos de seguridad de la información del activo.

Muchas organizaciones nunca han tomado un inventario preciso y completo de sus activos de información. El hecho de no identificar a los propietarios de activos es una de las razones principales por las que la administración de la seguridad de la información a menudo es ineficaz en las organizaciones [38].

Actividad 6 - Determinar la Valoración del Activo de Información

Antes de que se puedan evaluar los riesgos para un activo de información, se debe conocer el valor tangible e intangible del activo.

Determinar el valor es un intento de capturar cuán importante es esta información para la organización, principalmente el valor derivado de su uso, pero también considerando el impacto de su pérdida o falta de disponibilidad [38].

4.6.1 Selección de activos a perfilar

Para la selección de activos principalmente se enfocó en los activos que intervienen en los procesos de recaudación y permisos; para la recopilación de información y cumplimiento de las actividades para perfilar un activo se respondió a las preguntas que se encuentran en el Anexo D, esto conjuntamente con el jefe del Departamento Tecnológico.

Los activos identificados son los siguientes:

1. Plataforma de Recaudo
2. Base de datos

3. Correo electrónico
4. Digitalizador de Documentos
5. Documentos
6. Intranet
7. Directorio activo
8. Servidor de aplicaciones
9. Servidor de desarrollo
10. Servidor de pruebas

4.6.2 Creación de Perfiles de Activos Seleccionados

4.6.2.1 Perfilamiento del activo Plataforma de recaudo

Perfil de activos de información		
Activo Critico:	Plataforma de recaudo.	
Descripción: Es una modulo incluido en el sistema Cabildo, los contribuyentes realizan los pagos de las obligaciones con la municipalidad (agua, impuestos, permisos)		
Fecha de creación:	15/01/2019	
Titular del activo:	Jefe de Departamento Tecnológico.	
Contenedores para los activos de información		
Hardware:	Servidor de aplicaciones.	
Requerimientos de seguridad		
Confidencialidad: Solo el administrador y los empleados tienen el acceso al sistema con un usuario y contraseña única asignada por el administrador Ing. Luis Carrasco.		
Integridad: La información que se muestra en la plataforma de recaudo debe ser verídica y confiable.		
Disponibilidad: La plataforma de recaudo debe estar disponible durante las 8 horas de atención.		
Valoración:		
Confidencialidad:	Integridad:	Disponibilidad: X
La plataforma debe estar disponible ya que de no ser así provoca molestias a los contribuyentes.		

Tabla 19 Perfilamiento del activo Plataforma de recaudo

Fuente: Elaboración propia

4.6.2.2 Perfilamiento del activo Bases de datos

Perfil de activos de información		
Activo Critico:	Bases de datos	
Descripción: Esta alojada en el servidor de base de datos está vinculada a todos los módulos de los sistemas del GAD Municipal de Pelileo en ella se guarda toda la información digital de la institución.		
Fecha de creación:	15/01/2019	
Titular del activo: Jefe de Departamento Tecnológico		
Contenedores para los activos de información		
Hardware:	Servidor de bases de datos.	
Requerimientos de seguridad		
Confidencialidad: El administrador y a la vez jefe del Departamento Tecnológico Ing. Luis Carrasco es el único que puede ingresar o dar permiso para ingresar a la base de datos y realizar cualquier tipo de modificación.		
Integridad: La información de las distintas áreas que utilizan sistemas en la municipalidad deben ser almacenada en las bases de datos solo si la información es verifica y de fuente confiable.		
Disponibilidad: La información que se encuentra almacenada en las bases de datos debe estar siempre disponible ya que en ella se encuentra la información tanto del contribuyente como de toda la municipalidad, pagos, deudas, informes, etc.		
Valoración:		
Confidencialidad**:**	Integridad:	Disponibilidad: X
Las bases de datos tienen que estar siempre disponible, en jornada laboral para almacenar cualquier trámite pertinente (recaudación, permiso) y fuera de la jornada laboral por si algún contribuyente quiere realizar una consulta en el portal web de la institución.		

Tabla 20 Perfilamiento del activo Bases de datos

Fuente: Elaboración propia

Los perfiles de los activos de información restantes se encuentran en el Anexo D.

4.6.3 Identificar los Contenedores de los Activos Informáticos

En este se identifica los repositorios donde se procesa, transporta y almacena información de la institución, normalmente es donde se pueden producir ataques y

robos de información aquí es donde se debe enfatizar realizar un control de seguridad [39].

Para el presente proyecto se identificaron los siguientes contenedores de información.

Nombre- Descripción	Propietario
Data center: Instalación física en donde se encuentran los servidores y distribución de la red interna.	Jefe de Departamento Tecnológico

Tabla 21 Contendor data center

Fuente: Elaboración propia

Nombre - Descripción	Propietario
Bases de datos: Banco de datos que almacenan la información de la entidad	Jefe de Departamento Tecnológico

Tabla 22 Contendor bases de datos

Fuente: Elaboración propia

Nombre- Descripción	Propietario
Plataforma de correo: Correo electrónico corporativo de la entidad (Intranet).	Jefe de Departamento Tecnológico

Tabla 23 Contendor plataforma de correo

Fuente: Elaboración propia

Nombre- Descripción	Propietario
Directorio Activo: Servicio que almacena datos personales de los empleados, así como los roles, usurarios y contraseñas asignadas al personal del GAD.	Jefe de Departamento Tecnológico

Tabla 24Contendor directorio activo

Fuente: Elaboración propia

Nombre- Descripción	Propietario
Servidor de aplicaciones: Servidor donde se alojan las aplicaciones Core del negocio tales como Microsoft Office, Cabildo, Aplicativo web, Pagina Digitalizador de Documentos, Intranet, Antivirus	Jefe de Departamento Tecnológico

Tabla 25 Contendor servidor de aplicaciones

Fuente: Elaboración propia

Nombre- Descripción	Propietario
Servidor de desarrollo: Servidor donde se tiene instalado los entornos de desarrollo.	Jefe de Departamento Tecnológico e ingeniero encargado de desarrollo.

Tabla 26 Contendor interno servidor de desarrollo

Fuente: Elaboración propia

Nombre- Descripción	Propietario
Servidor de pruebas: Servidor donde se pruebas las aplicaciones y módulos desarrollados en la entidad. Además, se prueban aplicaciones de terceros que se desea utilizar en la institución.	Integrantes del Departamento Tecnológico

Tabla 27 Contendor servidor de pruebas

Fuente: Elaboración propia

Nombre- Descripción	Propietario
USB: Dispositivo de almacenamiento interno y externo que se utiliza entre las diferentes áreas para enviar archivos de gran volumen	Personal autorizado, gerentes de áreas

Tabla 28 Contendor USB

Fuente: Elaboración propia

Contenedor interno	
Nombre- Descripción	**Propietario**
Disco Duro: Dispositivos que almacenan información y backup de la institución.	Jefe de Departamento Tecnológico

Tabla 29 Contendor disco duro

Fuente: Elaboración propia

Contenedor interno	
Nombre- Descripción	**Propietario**
Computador: Dispositivos portátiles o PC asignados a los empleados de la entidad.	Personal de cada área del GAD de San Pedro de Pelileo

Tabla 30 Contendor computador

Fuente: Elaboración propia

Contenedor interno	
Nombre- Descripción	**Propietario**
Repisas, anaqueles, armarios, escritorios: Documentos físicos del municipio.	Personal de cada área del GAD de San Pedro de Pelileo

Tabla 31 Contendores Repisas, anaqueles, armarios, escritorios

Fuente: Elaboración propia

4.7 Identificación y evaluación de vulnerabilidades de componentes críticos

4.7.1 Identificar las áreas de preocupación

Para este paso se realizó una reunión con el Ing. Julio Flores representante del Departamento Tecnológico y con el Técnico profesional de riesgos Ing. Wilson Llerena que pertenece al Departamento de Servicios Públicos, en donde se procedió a realizar un análisis de situaciones que podrían afectar o poner en riesgo los activos de información y posteriormente se procedió a elegir las áreas de preocupación que se muestran la siguiente tabla.

Activos de información	Áreas de Preocupación
1. Plataforma de Recaudo 2. Base de datos 3. Correo electrónico 4. Digitalizador de Documentos 5. Documentos 6. Intranet 7. Directorio activo 8. Servidor de aplicaciones 9. Servidor de desarrollo 10. Servidor de pruebas	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.
	Exposición de los activos de información, acceso no autorizado a la infraestructura física.
	Desconocimiento en el manejo de los sistemas o equipos informáticos
	Interrupción en el servicio de energía electrónica
	Problemas de conectividad en la red interna de la organización
	Interrupción en el servicio de internet
	Falla en los componentes de hardware en los equipos informáticos
	Actualización o instalación de software sin autorización
	Desastres naturales
	Fallo o defecto de software

Tabla 32 Áreas de preocupación

Fuente: Elaboración propia

Una vez que se identificaron las áreas de preocupación se procede a detallar cada área de preocupación con el activo correspondiente en donde debe constar ¿quién puede

realizar la acción?, ¿por qué medio se puede dar?, ¿Qué motivos puede tener?, ¿En que se puede afectar a la institución? y ¿Qué requisito de seguridad debería tener?
Hay que mencionar que algunas combinaciones de áreas de amenaza con activo no pueden resultar una amenaza real para la entidad, por lo que podrían descartar, pero por perdido del jefe del departamento tecnológico se realizara el análisis de todas [37].

4.7.1.1 Análisis de las áreas de preocupación para el activo Plataforma de recaudo

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales			
Resultados:	Divulgación: X	Modificación:	Destrucción:	Interrupción:
Requisito de seguridad:	Solo los usuarios autorizados podrán ingresar a la plataforma de recaudo y realizar los cobros o actividades correspondientes.			

Tabla 33 Activo Plataforma de Recaudo, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo las personas del área de tecnologías pueden ingresar a la infraestructura física.			

Tabla 34 Activo Plataforma de Recaudo, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Ingreso a la plataforma de recaudo			
Motivos:	Intereses personales, divulgación información, falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: x
Requisito de seguridad:	Solo el personal encargado de recaudo y los del área de tecnología pueden ingresar al sistema, ya que son los únicos que cuentan con usuario y contraseña.			

Tabla 35 Activo Plataforma de Recaudo, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Interrupción en el servicio de energía eléctrica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción x
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 36 Activo Plataforma de Recaudo, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Problemas de conectividad en la red interna de la organización.			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la Organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La plataforma de recaudo no estará disponible si hay problemas en la red hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 37 Activo Plataforma de Recaudo, área de preocupación Problemas de conectividad en la red interna de la organización
Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 38 Activo Plataforma de Recaudo, área de preocupación Interrupción en el servicio internet

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico debe manipular los dispositivos informativos, y si existe alguna falla en el equipo el usuario debe dar aviso para la revisión respectiva.			

Tabla 39 Activo Plataforma de Recaudo, área de preocupación Falla en los componentes de hardware en los equipos informáticos.
Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El usuario no debe realizar las actualizaciones o modificaciones al sistema ese puede provocar la detención de servicios, el departamento tecnológico es el encargado de realizar estas acciones.			

Tabla 40 Activo Plataforma de Recaudo, área de preocupación Actualización o instalación de software sin autorización.
Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climatológicos.			
Resultados:	Divulgación:	Modificación	Destrucción: X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 41 Activo Plataforma de Recaudo, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Plataforma de recaudo			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación Falla del sistema por actualizaciones.			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El sistema de recaudo se detendrá hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 42 Activo Plataforma de Recaudo, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

4.7.1.2 Análisis de las áreas de preocupación para el activo Base de Datos

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos			
Actor:	Personal interno			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	La base de datos no se podrá utilizar hasta realizar un restablecimiento de información del ultimo backup realizado.			

Tabla 43 Activo Base de Datos, Exposición de los activos de información, acceso no autorizado a los sistemas informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado			
Motivos:	Intereses personales			
Resultados:	Divulgación	Modificación:	Destrucción	Interrupción: X
Requisito de seguridad:	Solo las personas del área de tecnologías pueden ingresar a la infraestructura física donde se encuentran los servidores.			

Tabla 44 Activo Base de datos, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	personal interno y externo			
Medio:	Ingreso a la base de datos			
Motivos:	Intereses personales, divulgación información, substracción de información			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: x
Requisito de seguridad:	Solo personal autorizado puede ingresar a la base de datos mediante usuarios y contraseñas otorgadas por el jefe de departamento tecnológico.			

Tabla 45 Activo Base de datos, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Interrupción en el servicio de energía electrónica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 46 Activo Base de datos, área de preocupación Interrupción en el servicio de energía electrónica

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales, daño a la organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La base de datos no estará disponible si hay problemas en la red hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 47 Activo Base de datos, área de preocupación Problemas de conectividad en la red interna de la organización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: x
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 48 Activo Base de datos, área de preocupación Interrupción en el servicio internet

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: x
Requisito de seguridad:	Solo el departamento tecnológico debe manipular y realizar revisiones de la base de datos, en caso de presentar falla el servicio de base de datos se detendrá hasta identificar y solucionar el problema.			

Tabla 49 Falla en los componentes de hardware en los equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de sistema o algún componente de la base de datos primero se debe realizar una evaluación en el servidor de pruebas para verificar si funciona correctamente.			

Tabla 50 Activo Base de datos, área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Causas naturales			
Resultados:	Divulgación:	Modificación:	Destrucción: X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 51 Activo Base de datos, área de preocupación Desastres naturales

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Base de datos			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La base de datos detendrá el funcionamiento hasta que los encargados del departamento tecnológico encuentren el fallo y reanuden el servicio.			

Tabla 52 Activo Base de datos, área de preocupación Falla o defecto de software

Fuente: Elaboración propia

La identificación de las áreas de preocupación del resto de activos de información se encuentra en el Anexo E.

4.7.2 Identificar Escenarios de Amenaza

Los escenarios de amenaza para casi todas las instituciones son prácticamente los mismos y se clasifican por grupos, como se puede observar en la Tabla 50.

En este paso lo importante es interpretar a que escenario de amanezca pertenece las áreas de preocupación que se eligieron anteriormente y que impacto (divulgación, modificación, destrucción o interrupción) tiene sobre la entidad, esto se realiza para cada activo.

Cabe recalcar que para este paso es de suma importancia que el análisis de áreas de preocupación se de cada activo estén realizadas correctamente ya que de ahí se obtienen los datos para los escenarios de amenaza.

Árbol de Amenaza	Descripción
Actores humanos utilizado medios técnicos	Esta categoría se refiere a las amenazas a los activos de información realizadas por un actor humano de forma directa sea accidental o deliberada a la infraestructura técnica de la organización.
Actores Humanos utilizando acceso físico.	Esta categoría se refiere a las amenazas a los activos de información realizadas por un actor humano por acceso físico de manera directa o sobre su contenedor sea accidental o deliberada a la organización.
Problemas técnicos	Esta categoría se refiere a las amenazas a los activos de información por problemas con la tecnología y los sistemas de información de la organización. Incluye los defectos de hardware, software, virus y otros problemas relacionados con el sistema.
Otros	Esta categoría se refiere a las amenazas a los activos de información son los problemas o situaciones que están fueran del alcance de control de la organización. Incluye los desastres naturales (inundaciones, terremotos, incendios, erupciones volcánicas) y los riesgos de interdependencia por ejemplo fuente de alimentación eléctrica.

Tabla 53 Escenarios de amenaza [37]

Fuente: Elaboración propia

4.7.2.1 Escenarios de amenaza del activo plataforma de recaudo

Activo de Información Plataforma de Recaudo		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Interrupción
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Interrupción
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 54 Escenarios de amenaza del activo plataforma de recaudo

Fuente: Elaboración propia

4.7.2.2 Escenarios de amenaza del activo Base de datos

Activo de Información: Base de datos		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Interrupción

Activo de Información: Base de datos		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 55 Escenarios de amenaza del activo Base de Datos

Fuente: Elaboración propia

La identificación de los escenarios de amenaza del resto de activos de información se encuentra en el Anexo F.

4.8 . Análisis de riesgos de los activos de TI

4.8.1 Identificación de Riesgos

Si se cumple el escenario de amenaza en un activo puede traer una o más consecuencias a la institución y por ende estos son los riesgos podrían afectar a la institución.

Riesgo = (Áreas de Preocupación y Escenarios de Amenaza) +Consecuencias [37].

Se realiza la identificación de riesgos para cada escenario de amenaza de los activos de información elegidos.

4.8.1.1 Consecuencias de la Plataforma de recaudo

Activo de Información: Plataforma de recaudo	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	- Los integrantes del departamento deberán verificar las ultimas movimientos en la base de datos que vinieron por parte del sistema de recaudación. -En caso de que existan modificaciones que no sean coherentes, se deberán realizar una restauración de la copia de seguridad para regresar a un estado anterior.
Desconocimiento en el manejo de los sistemas informáticos	-Los usuarios que realizan la recaudación tendrán contratiempos al cobrar a los contribuyentes lo que presentara molestias y pérdida de tiempo.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-La plataforma de recaudo no podrá ser abierta hasta que se verifique si se realizó alguna modificación o se alteró algún elemento del servidor donde está alojado la plataforma.
Problemas de conectividad en la red interna de la organización	-La plataforma de recaudo no estará disponible generando molestias en los contribuyentes que quieran realizar los pagos. -Los miembros del departamento tecnológico tendrán que encontrar la falla y restablecer el servicio retrasando actividades que tenían planeadas para la jornada laboral.
Interrupción en el servicio de internet	-La plataforma de recaudo seguirá funcionando en la institución, pero si algún contribuyente por medio de la página web quiere consultar el valor que desea pagar no podrá realizarlo.

Activo de Información: Plataforma de recaudo	
Escenario de amenaza	**Consecuencia**
Falla en los componentes de hardware de los equipos	- La ventanilla de recaudación que presenta el problema no estará operando generando malestar y contratiempos tanto para contribuyentes como para los empleados.
Actualización o instalación de software sin autorización	-La plataforma de recaudo puede presentar incompatibilidad con la actualización y puede dejar de funcionar.
Fallo o defecto de Software	-Los empleados del lugar donde se presenta la falla dejan de laborar hasta que el departamento tecnológico encuentre la falla, generando molestia tanto en el empleado como en los contribuyentes.
Interrupción en el servicio de energía eléctrica	-La plataforma de pago no estará disponible hasta restablecer la energía eléctrica.
Desastres Naturales	- La Plataforma de recaudo no estará disponible si un desastre natural ocurre.

Tabla 56 Consecuencias de la Plataforma de recaudo

Fuente: Elaboración propia

4.8.1.2 Consecuencias de la base de datos

Activo de Información: Base de datos	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	- Los integrantes del departamento tecnológico deben verificar si existieron modificaciones en la base de datos durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenían planificadas. -En el caso de encontrar alguna alteración de la base de datos deberán realizar un restablecimiento de la última copia de seguridad almacenada, además se tendrían que dar el trabajo de verificar las acciones que se realizaron correctamente durante la exposición y añadirlas a la base de datos.

Activo de Información: Base de datos	
Escenario de amenaza	**Consecuencia**
Desconocimiento en el manejo de los sistemas informáticos	-Los empleados de distintas áreas del municipio tienen dificultad para realizar una consulta a la base de datos desde el sistema que utiliza presentando retraso en las actividades que realiza. -El empleado que presente dificultad solicita asistencia al área de departamento tecnológico quienes deberán dirigirse a el área de trabajo solicitada dejando de lado actividades que estaba realizando.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	- La base de datos estará temporalmente inhabilitada hasta que se verifique si se realizó alguna modificación o se alteró algún elemento del servidor donde está alojado, esto presentara fallo a todo el municipio ya que gran parte de las aplicaciones dejaría de funcionar al no tener en donde guardar o consultar información.
Problemas de conectividad en la red interna de la organización	-La base de datos no tendría conexión con los sistemas, por lo tanto, se suspenderán los servicios del municipio generando retrasos y perjuicios para la institución.
Interrupción en el servicio de internet	-La base de datos estará disponible internamente, pero para consultas de la página web estará fuera de servicio mientras se restablece la conectividad a internet.
Falla en los componentes de hardware de los equipos	-La base de datos se inhabilitará hasta que los encargados identifiquen y reparen el fallo, por lo que las actividades de las áreas que utilicen aplicativos que interactúen directamente con la base de datos verán interrumpidas sus actividades, generado pérdidas y retrasos en la institución.

Activo de Información: Base de datos	
Escenario de amenaza	**Consecuencia**
Actualización o instalación de software sin autorización	- La base de datos puede presentar incompatibilidad con la actualización realizada y presentar fallos.
Fallo o defecto de Software	-Las actividades de las áreas que utilizan sistemas que se conectan a la base de datos tienen que detenerse hasta que el departamento tecnológico solucione el problema.
Interrupción en el servicio de energía eléctrica	--La base de datos estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	- La base de datos no estará disponible si un desastre natural ocurre.

Tabla 57 Consecuencias de las bases de datos

Fuente: Elaboración propia

La identificación de riesgos del resto de activos de información se encuentra en el Anexo G.

4.8.2 Análisis de Riesgos

Teniendo los posibles riesgos en la institución se procede a realizar un análisis cuantitativo para cada activo de información en donde se podrá observar cuan afectada seria la entidad si se produjera dichos riegos, la información obtenida ayuda a determinar que riesgos deben ser tratados con mayor prioridad.

Para realizar el análisis de riesgos se utilizarán los escenarios de amenaza de cada activo, el criterio de evaluación con la respectiva prioridad que se definió inicialmente en el proceso y un valor de impacto del riesgo a la organización (Alto (3), Medio (2) y Bajo (1)) definido el auditor.

El cálculo se realizó multiplicando el valor de prioridad del criterio de evaluación con valor de impacto asignado posteriormente se realiza la suma de estos valores.

Finalmente se realizó una tabla de resumen de cada activo con el puntaje de cada área de preocupación y se asignó el impacto que se produce a la entidad de acuerdo a la puntuación obtenida.

Impactos de área de Preocupación		
30 a 45	**16 a 29**	**0 a 15**
Alto	Medio	Bajo

Tabla 58 Impactos de área de Preocupación
Fuente: Elaboración propia

4.8.2.1 Análisis de riesgos de la Plataforma de Recaudo

Área de preocupación	**Criterio de evaluación**	**Prioridad**	**Valor del impacto**	**Puntuación**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 59 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos
Fuente: Elaboración propia

Área de preocupación	**Criterio de evaluación**	**Prioridad**	**Valor del impacto**	**Puntuación**
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 60 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.
Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 61 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Baja (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 62 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			35

Tabla 63 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Interrupción en el servicio de internet.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 64 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 65 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 66 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Fallo o defecto de Software.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 67 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Interrupción en el servicio de energía eléctrica.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			38

Tabla 68 Análisis de riesgos de la Plataforma de Recaudo en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del Activo Plataforma de Recaudo		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Medio	24
Desconocimiento en el manejo de los sistemas informáticos.	Medio	24
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	24
Problemas de conectividad en la red interna de la organización.	Medio	19
Interrupción en el servicio de internet	Alto	35

Resumen de áreas de Preocupación del Activo Plataforma de Recaudo		
Área de preocupación	**Impacto**	**Puntaje**
Falla en los componentes de hardware de los equipos	Medio	24
Actualización o instalación de software sin autorización	Medio	24
Fallo o defecto de Software	Medio	24
Interrupción en el servicio de energía eléctrica.	Alto	33
Desastres Naturales	Alto	38

Tabla 69 Resumen de las áreas de preocupación del activo Plataforma de Recaudo

Fuente: Elaboración propia

4.8.2.2 Análisis de riesgos de la Base de Datos

Área de preocupación	**Criterio de evaluación**	**Prioridad**	**Valor del impacto**	**Puntuación**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 70 Análisis de riesgos de la Base de Datos en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	**Criterio de evaluación**	**Prioridad**	**Valor del impacto**	**Puntuación**
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Baja (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 71 Análisis de riesgos de la Base de Datos en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Alto (3)	15
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Baja (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			29

Tabla 72 Análisis de riesgos de la Base de Datos en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 73 Análisis de riesgos de la Base de Datos en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 74 Análisis de riesgos de la Base de Datos en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 75 Análisis de riesgos de la Base de Datos en el área de preocupación Falla en los componentes de hardware de los equipos

Fuente: Elaboración propia

Área de preocupación	Área de impacto	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Alto (3)	15
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			29

Tabla 76 Análisis de riesgos de la Base de Datos en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			36

Tabla 77 Análisis de riesgos de la Base de Datos en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 78 Análisis de riesgos de la Base de Datos en el área de preocupación Interrupción en el servicio de energía eléctrica.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			38

Tabla 79 Análisis de riesgos de la Base de Datos en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del Activo Base de Datos		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Medio	24
Desconocimiento en el manejo de los sistemas informáticos.	Medio	24
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	29
Problemas de conectividad en la red interna de la organización.	Alto	33

Resumen de áreas de Preocupación del Activo Base de Datos		
Área de preocupación	**Impacto**	**Puntaje**
Interrupción en el servicio de internet	Alto	33
Falla en los componentes de hardware de los equipos	Medio	28
Actualización o instalación de software sin autorización	Medio	29
Fallo o defecto de Software	Alto	36
Interrupción en el servicio de energía eléctrica.	Alto	33
Desastres Naturales	Alto	38

Tabla 80 Resumen de las áreas de preocupación del activo Base de Datos

Fuente: Elaboración propia

El análisis de riesgos del resto de activos de información se encuentra en el Anexo H. Con el análisis e interpretación de información y la aplicación de la metodología se da fiel cumplimiento a lo estipulado en el segundo objetivo específico de esta investigación.

4.9 Enfoque de mitigación

Se determinan que riesgos requieren ser tratados y se desarrolla una estrategia de mitigación para esos riesgos. Esto se logra priorizando primero los riesgos según su puntaje de riesgo relativo. Una vez que se han priorizado los riesgos, se desarrollan estrategias de mitigación que tienen en cuenta el valor del activo y sus requisitos de seguridad, los contenedores en los que se almacenan y el entorno operativo de la organización. [37]

La probabilidad es necesaria para determinar que escenarios son más propensos a ocurrir, en este caso se consideró la probabilidad subjetiva debido a que en la mayoría de los casos no existe un registro o control de las ocurrencias presentadas.

Valor	**Frecuencia**
Alto	Más de 5 veces al año
Medio	De 2 a 4 veces al año
Bajo	1 vez al año

Tabla 81 Probabilidad subjetiva de amenaza

Fuente: [40]

En OCTAVE se puede hacer uso de la matriz de riesgo relativo, un elemento que permite visualizar los riesgos a tratar con base en la probabilidad y el puntaje de riesgo. Se categorizan grupos de escenarios de amenazas para su tratamiento con base en estos resultados, como se muestra en la siguiente imagen. Los riesgos que pertenecen al grupo 1 deberían ser tratados con mayor prioridad:

Matriz de riesgos relativos			
Probabilidad	Puntaje de riesgo		
	30 a 45	**16 a 29**	**0 a 15**
Alta	Grupo 1	Grupo 2	Grupo 2
Media	Grupo 2	Grupo 2	Grupo 3
Baja	Grupo 3	Grupo 3	Grupo 4

Tabla 82 Matriz de riesgos relativos

Fuente: [41]

Según el grupo al que pertenece el riesgo se realiza el enfoque de mitigación:

Grupo	**Enfoque de Mitigación**
Grupo 1	Mitigar
Grupo 2	Mitigar o Transferir
Grupo 3	Transferir o Aceptar
Grupo 4	Aceptar

Tabla 83 Enfoque de mitigación según el grupo

Fuente: [40]

4.9.1 Mitigación de riesgo del activo Plataforma de Recaudo

Nombre del activo:	Plataforma de recaudo		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 24	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Plataforma de recaudo</td></tr>
<tr><td colspan="4">Control
Solo el jefe de departamento tecnológico y empleados encargados de cobro pueden acceder a la plataforma de recaudo.
El ingreso a la plataforma de recaudo debe realizarse solo con los usuarios y contraseñas asignadas.
El jefe de departamento tecnológico debe realizar el cambio de contraseñas mensualmente.
Los empleados no deben tener los usuarios y contraseñas expuestos o visibles (notas, documentos, archivos).</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar un manual de usuario que muestre como utilizar cada una de las acciones de la plataforma de recaudo.
Realizar capacitaciones a los usuarios de la plataforma de recaudo para que mejoren la productividad.</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar al data center y realizar modificaciones al servidor que está instalado la plataforma de recaudo.
Las computadoras que utilizan para realizar los cobros solo deben ser manipuladas por usuario y los integrantes del departamento tecnológico.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Plataforma de recaudo</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna.
Configurar restricciones de firewall para que las PC encardas de recaudo tengan acceso solo a los servicios necesarios.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos a los equipos.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente. Memoria RAM, disco duro, cables)
Adquirir repuestos compatibles con los equipos y con proveedores de confianza.</td></tr>
</table>

<table>
<tr><td colspan="2">Nombre del activo:</td><td colspan="2">Plataforma de recaudo</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el personal de departamento tecnológico puede instalar y actualizar software.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.
Se debe comunicar a los empleados que no pueden instalar ningún software.
El departamento debe crear cuentas exclusivas en los ordenadores de los empleados que solo tengan los permisos necesarios.
Instalar frezzeadores para que si instalan alguna aplicación al reiniciar la PC no se vea afectado.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 36</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos preventivos en los equipos que utilizan la plataforma de recaudación.
Realizar actualizaciones del sistema previo análisis en el servidor de pruebas.
Deshabilitar los servicios del ordenador que no sean necesarios.
Planificar configuración de Servidores
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción:
Mitigar</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Plataforma de recaudo</td></tr>
<tr><td colspan="4">Control:
Adquirir un UPS exclusivo para el servidor de aplicaciones y así evitar daños, ya que en este se aloja los servicios necesarios para la plataforma de recaudación.
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.</td></tr>
<tr><td colspan="4">Área de preocupación: Desastres Naturales</td></tr>
<tr><td>Puntaje de riesgo relativo: 38</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar respaldo de información de los datos de la plataforma de recaudo y almacenarlos en la nube.
Crear un plan estratégico en caso de desastres naturales.
Mejorar la señalización en las oficinas que se realizan los cobros.
Tener equipos en contra de incendios ubicados en lugares estratégicos.</td></tr>
</table>

Tabla 84 Mitigación de riesgo del activo Plataforma de Recaudo

Fuente: Elaboración propia

4.9.2 Mitigación de riesgo del activo Base de Datos

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Base de datos</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo:24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico debe tener acceso a la administración de la base de datos.
Solo se puede ingresar a la base de datos con un usuario y contraseña.
El jefe de departamento tecnológico debe realizar el cambio de contraseñas mensualmente, las contraseñas deben ser al menos 18 caracteres (letras mayúsculas y minúsculas, números, símbolos).
Realizar diariamente copias de seguridad.
Realizar un log que almacene el historial de los cambios que se realizó en la base de datos en el que conste usuario, fecha, hora, cambio.</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el jefe del departamento tecnológico puede realizar cambios en la base de datos, en caso de requerir asistencia debe estar presente para verificar las modificaciones que se realicen.
Se debe realizar un instructivo en que debe constar los cambios que se realiza en la base de datos.
Se debe crear un instructivo para los usuarios de las distintas áreas en caso de que realicen una consulta de información a la base de datos.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Base de datos</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 29</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center, pero solo el jefe del departamento puede realizar modificaciones donde se encuentra la base de datos.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna.
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Base de datos</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos a los servidores.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente, procesador. Memoria RAM, disco duro, cables)</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo: 29</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico puede instalar y actualizar un componente de la base de datos.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo:36</td><td>Probabilidad subjetiva: Alto</td><td>Categoría: Grupo 1</td><td>Acción: Mitigar</td></tr>
<tr><td colspan="4">Control:
Comprar Oracle en su versión completa o migras a una base de datos libre.
Planificar configuración de Servidores.
Realizar actualizaciones del sistema previo análisis en el servidor de pruebas.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.
Desinstalar los programas que no sean necesarios para la correcta funcionalidad de las bases de datos.
Antes de instalar actualizaciones de nuevas versiones de gestor de base de datos se debe realizar pruebas y estudios de compatibilidad y carga.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Base de datos</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo: 36</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción:
Mitigar</td></tr>
<tr><td colspan="4">Control:
Adquirir un UPS exclusivo para el servidor de base de datos y así evitar daños, ya que en este se almacena toda la información del GAD Municipal de Pelileo
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.</td></tr>
<tr><td colspan="4">Área de preocupación: Desastres Naturales</td></tr>
<tr><td>Puntaje de riesgo relativo: 36</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar respaldo de la base de datos y almacenarlos en la nube.
Crear un plan estratégico en caso de desastres naturales.
Mejorar la señalización en el departamento tecnológico.
Tener equipos en contra de incendios ubicados en lugares estratégicos</td></tr>
</table>

Tabla 85 Mitigación de riesgo del activo Base de Datos

Fuente: Elaboración propia

La mitigación de riesgos del resto de activos de información se encuentra en el Anexo I.

Con las recomendaciones realizadas para tener un mejor uso de las TI, mejorar la seguridad e integridad de la información y la reducción de riesgos que se podrían dar en la entidad, se da por cumplido el tercer objetivo específico de esta investigación.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Mediante el estudio inicial de la entidad pública mediante antecedentes e información obtenida por distintos medios, se logró tener una idea mas clara de lo que esta ocurriendo en la institución y en que puntos se debe poner mayor énfasis.
- Los procesos de permisos y recaudación del municipio de Pelileo esta ligados directamente, por este motivo el tutor de la entidad solicito el análisis de únicamente de los activos que intervienen en estos procesos, si bien se encontraron puntos altos estos podrían mejorarse.
- La aplicación de la Auditoria Informática bajo la metodología OCTAVE fue de gran utilidad, ya que permitió enfocarse en los activos de información que intervenían en los procesos, contemplando varios escenarios de amenazas y así tener un mayor alcance en la identificación e evaluación de los riesgos,
- Las instalaciones físicas no cuentan con seguridad de registro de acceso al lugar o cámaras de vigilancia, lo que pone en riesgo a departamento tecnológico donde se encuentra el centro de procesamiento de datos.
- Al realizar la auditoria se identificó que el GAD municipal actualmente utiliza una versión de prueba de Oracle lo que limita funciones y espacio de almacenamiento, que en un futuro sería necesario por la cantidad de información que se maneja en la entidad.
- Al realizar la mitigación de riesgos se procedió a dar recomendaciones entre ellas los controles que se deben realizar para evitar que un riesgo se materialice, siempre contemplando que vaya encaminado a tener una mayor seguridad e integridad de la información.

- El Informe Final de Auditoría será dirigido al jefe del Departamento Tecnológico quien tomará la decisión de aplicar las recomendaciones con el fin de mejorar la condición de las instalaciones físicas y asegurar que la información institucional.

5.2 Recomendaciones

Una vez culminado el proyecto de investigación se tiene las siguientes recomendaciones:

- Se recomienda realizar frecuentemente una análisis y evaluación informática de la institución para saber en qué situación se encuentra y verificar si existen falencias en el uso de las TI.
- Se recomienda realizar documentación de los procesos de tecnologías de la información (TI), para que con un análisis se puedan definir controles de seguridad de la información y así evitar vulnerabilidades frente a pérdidas de información por accesos no autorizados de personal ajeno a la institución.
- Se recomienda adecuar las instalaciones del área de informática en especial en donde se encuentran los servidores ya que el lugar no cuenta con una seguridad adecuada, además plantear la instalación de cámaras de seguridad.
- Se recomienda al Jefe de Departamento Tecnológico realice gestiones con GAD Municipal de Pelileo para adquirir la licencia de Oracle o a su vez realizar un proyecto para migrar a una base de datos libre.
- Se debería impartir cursos de capacitaciones y evaluaciones de los usuarios de los sistemas del GAD Municipal de Pelileo, para mejorar el desempeño diario en las actividades de la institución y así alcanzar los objetivos de la institución.
- Se recomienda realizar una Auditoria Informática a todo el GAD Municipal de San Pedro de Pelileo y no solo departamentos específicos.
- El jefe de Departamento Tecnológico del GAD Municipal de San Pedro de Pelileo, debería considerar aplicar lo antes posible las recomendaciones del enfoque de mitigación a los procesos cuyo puntaje de riesgos relativo pertenezcan a los grupos 1 y 2 ya que en estos se presentan las mayores vulnerabilidades.

BIBLIOGRAFÍA

[1] R. Martínez, «¿Como reducir el factor humano en la seguridad informática de una empresa?,» iProfesional, 2018.

[2] D. TECNO, «La seguridad de la tecnología de la información es clave para un negocio exitoso,» Universo, 2018.

[3] F. Sandoval, «En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario,» El Telégrafo, Guayaquil, 2016.

[4] G. Sebastian, «Modelo ISO 27002, ITIL, COBIT,» *Escuela Politecnica del Ejercito (ESPE)* .

[5] G. Victor, «Evaluación de la Seguridad de la Información con la Metodología Octave».

[6] G. Vanegas y P. C, «Hacia un modelo para la gestión de riesgos de TI en,» *Revista S&T*, pp. 38-39, 2014.

[7] L. Ing.Carrasco, Interviewee, *Auditorias Internas GAD Municipal de San Pedro de Pelileo.* [Entrevista]. 11 02 2019.

[8] S. Torres y J. Rojas, Modelo De Gestión De Riesgos Aplicando Metodología Octave Allegro En Entidades Del Sector Fiduciario, Bogota, 2017.

[9] P. Crespo, Metodología De Seguridad De La Información Para La Gestión Del Riesgo Informático Aplicable A Mpymes, Cuenca, 2016.

[10] F. Arévalo, "Elaboración Y Plan De Implementación De Políticas De Seguridad De La Información Aplicadas A Una Empresa Industrial De Alimentos, Cuenca, 2017.

[11] A. Mejía, Auditoría de Gestión Informática en el Área de las Tecnologías de la Información para el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón La Concordia, Santo Domingo, 2017.

[12] F. Guevara y G. Torres, Auditoria Informática al GAD Municipal de la Ciudad de Riobamba, Provincia De Chimborazo Del Período 2014, Riobamba, 2017.

[13] J. Ulloa, «Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo,» Ambato, 2017.

[14] Y. Carcelén, «Auditoria Informática Mediante la aplicación de la Metodología COBIT (Control Objectives for Information and Related Technology) en la compañía I COACH SERVICIOS Consulting & Training Cia. Ltda,» Ambato, 2015.

[15] A. Gutierrez, AUDITORÍA. UN ENFOQUE PRÁCTICO, Madrid: Paraninfo, 2014.

[16] H. Sandoval, «Introduccion a la Auditoria,» México, 2012.

[17] M. Riquelme, «Tipos De Auditoria,» *Web y Empresas*, 2017.

[18] I. Ramirez, «Fundamentos de Auditoria de Informática,» 21 Abril 2018. [En línea]. Available: https://ivanrjimenez74.wixsite.com/imagenreactiva/single-post/2018/04/21/Fundamentos-de-Auditoria-de-Inform%C3%A1tica. [Último acceso: 12 Julio 2018].

[19] Tecnologico de Tepeaca, «Auditoria Informática,» 2015.

[20] E. Villa, «TIPOS Y CLASES DE AUDITORIAS INFORMÁTICAS,» *ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO* .

[21] M. Baranda, «Objetivos de la Auditoría de los Sistemas de Información,» *Gestiopolis*, 2018.

[22] R. Gomez, D. Paez, Y. Donoso y A. Herrera, «Methodology and Governance of the IT Risk Management,» *Revista de Ingeniería*, p. 4, 2010.

[23] V. Goméz y A. Ospina, «Evaluación de la Seguridad de la Información con la Metodología OCTAVE,» *Departamento de Ingenieria, Institución Universitaria Pascual Bravo.*

[24] A. Abril, J. Pulido y J. Bohada, «Análisis de riesgos en seguridad de la Información,» Tunja, 2014.

[25] J. Peña, «Metodologías y Nomas para el Analisis de Riesgos,» de *Alintec IT Governance Consultans*, Monterrey.

[26] M. d. C. Crespo, «El Análisis de Riesgos dentro de una Auditoría Informática: Pasos y Posibles Metodologías,» 2013.

[27] J. Pacheco, «Sepa por qué los procesos de TI son importantes para ejecutar un negocio de manera eficiente,» *Heflo*, 2017.

[28] Universidad de Barcelona, «Seguridad de la información, un conocimiento imprescindible,» 2017.

[29] S. Moro, «Análisis y gestión de riesgos en un Sistema Informático,» 2015.

[30] M. Erb, «Gestión de Riesgo en la Seguridad Informática,» 2009.

[31] J. Montalvo, O. Reyes y J. Cuesta, La Provincia de Tungurahua en 1928, Ambato: Raza Latina, 1928, pp. 165-166.

[32] G. Dr.Moreno, REGLAMENTO ORGÁNICO FUNCIONAL Y POR PROCESOS DEL GOBIERNO AUTÓNOMO DESENTRALIZADO MUNICIPAL DE SAN PEDRO DE PELILEO, Pelileo, 2016.

[33] Recursos Humanos (GAD San Pedro de Pelileo), «Organigrama Intitucional,» Pelileo, 2019.

[34] GAD Municipal Pelileo, «MISIÓN Y VISIÓN INSTITUCIONAL,» [En línea]. Available: http://www.pelileo.gob.ec/index.php/contact-us.html.

[35] ISO27000, «Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002,» [En línea]. Available: http://www.iso27000.es/iso27002.html. [Último acceso: 2005].

[36] M. Mendoza, «8 pasos para hacer una evaluación de riesgos (parte I),» welivesecurit by ESET, 2014.

[37] R. Caralli, J. Stevens y L. Young, *Introducing OCTAVE Allegro:Improving the Information Security Risk,* Hanscom: SOFTWARE ENGINEERING INSTITUTE, 2007.

[38] J. Stevens, *Information Asset Profiling*, 2005.

[39] A. Doria, «RIESGOS Y CONTROL INFORMÁTICO,» 2014.

[40] A. Conza y L. Medrano, Análisis de Riesgos Informaticos y Elaboracion de un Plan de Contitnuidad para la educuación virtual CEC-EPN, 2015.

[41] M. Mendoza, «8 pasos para hacer una evaluación de riesgos (parte II),» de *welivesecurit by ESET*, 2014.

[42] Recursos Humanos(GAD San Pedro de Pelileo), «Distributivo de Personal GAD de San Pedro de Pelileo,» Pelileo, 2019.

ANEXOS

ANEXO A: Encuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Objetivo: Recolectar información de la utilización de TI y uso de la información por parte de los usuarios en el GAD Municipal de San Pedro de Pelileo.

Instructivo: Marque la opción que le parezca más conveniente.

1. **¿La seguridad de la información manejada en la institución es adecuada?**

Si ☐

No ☐

2. **¿La información es restringida a personas ajenas a la institución?**

Si ☐

No ☐

3. **¿Considerar que se debe mejorar el manejo de la información y los equipos informáticos en el GAD de San Pedro de Pelileo?**

SI ☐

No ☐

4. **¿Se realizan copias de seguridad de la información en la institución?**

Siempre ☐

Casi siempre ☐

Frecuentemente ☐

Nunca ☐

5. ¿Se establecen claves exclusivas para su área de trabajo?

Si ☐

No ☐

6. ¿Tiene registradas sus claves en lugares visibles a otros usuarios (Notas, archivos)?

Si ☐

No ☐

7. ¿Con que frecuencia se cambian sus claves de acceso en su puesto de trabajo?

Trimestralmente ☐

Semestralmente ☐

Anualmente ☐

Nunca ☐

8. ¿Han realizado auditorías Informáticas en su área de trabajo?

Si ☐

No ☐

9. ¿Cree que el sistema informático que utiliza es adecuado para sus funciones?

Si ☐

No ☐

10. ¿Con que frecuencia el sistema informático presenta fallas?

Siempre ☐

Casi siempre ☐

Frecuentemente ☐

Nunca ☐

ANEXO B: Entrevista

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Objetivo: Recolectar información de la utilización de TI en el GAD Municipal de Pelileo.

Fecha: _____

Entrevistado: Ing. Luis Carrasco **Entrevistador:** Oscar Silva

Cargo: jefe del Departamento Tecnológico

1. **¿El personal con el que cuenta el departamento tecnológico es el adecuado para cumplir las funciones designadas?**

……
……
……...

2. **¿El personal del área está capacitado para realizar las tareas que desempeñan?**

……
……
……...

3. **¿Se requiere de servicios de terceros para cumplir con las funciones del área?**

……
……
……...

4. **¿El área de informática cuenta con documentación donde establezca sus funciones?**

……

……

……...

5. ¿Cree usted que el presupuesto asignado por el GAD Municipal al área informática es el adecuado?

……

……

……...

6. ¿Cree que el espacio físico del departamento tecnológico es el adecuado?

……

……

……...

7. ¿En caso de no encontrarse Ud. quién asume sus funciones?

……

……

……...

8. ¿Existen algún plan para la seguridad de la información de la institución?

……

……

……...

9. ¿Con cuántos sistemas cuenta la institución y cual son sus funciones?

……

……

……...

10. ¿Tiene programado realizar mantenimientos a los equipos informáticos? ¿Con que frecuencia los realiza?

……
……
……

11. ¿Cree que se da el mantenimiento adecuado a los equipos?

……

……

……...

ANEXO C: Abreviaturas y Acrónimos

OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation (Evaluación de amenazas, activos y vulnerabilidades operacionalmente críticas)
GAD	Gobierno Autónomo Descentralizado
TI	Tecnologías de la Información
ISO	International Organization for Standardization (Organización Internacional de Normalización)
UPS	Uninterruptible power supply (Sistemas de alimentación ininterrumpida)

ANEXO D: Perfilamiento de Activos

Preguntas para el Perfilamiento de activos

- ¿Qué activos de información son de mayor valor para su organización?
- ¿Qué activos de información se utilizan en los procesos de recaudaciones y permisos?
- Qué activos de información, si se pierden, interrumpirían significativamente la capacidad de su organización para lograr sus objetivos.
- ¿Qué otros activos están estrechamente relacionados con estos activos?
- ¿Cuál es el nombre común para este activo de información (cómo las personas
- dentro de la organización se refieren a ella)?
- ¿Es este activo de información es lógico o físico?
- ¿Quién en la organización tiene la responsabilidad principal de este activo de información?
- ¿Quién es el propietario de los procesos de negocio donde se utiliza este activo de información?
- ¿De quién son los procesos de negocios que más dependen de este activo de información?
- ¿Quién sería responsable de establecer el valor (monetario o de otro tipo) de este activo de información?
- ¿Quién se vería más afectado si se comprometiera el activo de información?
- ¿Existen diferentes propietarios para los diferentes elementos de datos que componen el activo de información?

Perfilamiento de Activos

Perfilamiento del activo correo electrónico

Perfil de activos de información		
Activo Critico:	Correo electrónico	
Descripción: El correo electrónico es un medio de comunicación que permite a los empleados de la municipalidad comunicarse internamente con el fin de realizar solicitudes, consultas, peticiones, informaciones, etc.		
Fecha de creación:	15/01/2019	
Titular del activo:	Jefe de Departamento Tecnológico	
Contenedores para los activos de información		
Hardware:	Servidor de Aplicaciones.	
Requerimientos de seguridad		
Confidencialidad: Los correos electrónicos que se realizan entre empleados son dirigidos únicamente a las personas de interés.		
Integridad: La información recibida o enviada por correo electrónico debe ser exacta y correcta.		
Disponibilidad: El servicio de correo electrónico y la información que reside ahí debe estar disponible permanentemente para los usuarios de este medio, al menos en la jornada laboral.		
Valoración:		
Confidencialidad:	Integridad:	Disponibilidad: X
Los empleados de la entidad siempre deben tener acceso al servicio de correo electrónico interno.		

Tabla 86 Perfilamiento del activo correo electrónico

Fuente: Elaboración propia

Perfilamiento del activo Intranet

Perfil de activos de información	
Activo Critico:	Intranet
Descripción: Es una plataforma interna que tiene la entidad donde los empleados acceden a los distintos sistemas conectados a los servidores y a documentos internos.	
Fecha de creación:	15/01/2019

Perfil de activos de información		
Activo Critico:	Intranet	
Titular del activo:	Jefe de Departamento Tecnológico	
Contenedores para los activos de información		
Hardware:	Servidor Aplicaciones	
Requerimientos de seguridad		
Confidencialidad: Solo se tendrá acceso por medio de los roles, usuarios y contraseñas asignados por el jefe de Departamento Tecnológico.		
Integridad: Solo se podrá acceder mediante los usuarios asignados y no se podrán realizar modificaciones si n autorización.		
Disponibilidad: Debe estar siempre disponible ya que por este medio interactúan los sistemas y se transmite la información y todas las acciones a realizarse.		
Valoración:		
Confidencialidad:	Integridad:	Disponibilidad: X
La intranet debe estar disponible y accesible a todos los usuarios de la entidad al menos en la jornada laboral debido a que la productividad se vería afectada.		

Tabla 87 Perfilamiento del activo Intranet

Fuente: Elaboración propia

Perfilamiento del activo sistema del digitalizador de documentos

Perfil de activos de información	
Activo Critico:	Sistema Digitalizador de Documentos.
Descripción: Es un método para almacenar y convertir documentos físicos en digitales por medio de un escáner, solo se almacenan los documentos de mayor relevancia, principalmente se lo está aplicando en la secretaria del GAD.	
Fecha de creación:	15/01/2019
Titular del activo: jefe de Departamento Tecnológico, administrador de avalúos y catastros, secretaria, recursos humanos.	
Contenedores para los activos de información	
Hardware: Servidor de aplicaciones.	

Perfil de activos de información		
Activo Critico:	Sistema Digitalizador de Documentos.	
Requerimientos de seguridad		
Confidencialidad: Solo las personas que tengan autorización pueden digitalizar documentos y subirlos al sistema para ello solo se dispone de un usuario y contraseña.		
Integridad: Los empleados de acuerdo al rol asignado tendrá la opción de agregar, modificar o solo revisarlo los documentos.		
Disponibilidad: Los documentos que se encuentran en esta plataforma deben estar siempre disponibles en el caso que algún empleado requiera consultarlos o utilizarlo.		
Valoración:		
Confidencialidad**: X**	Integridad:	Disponibilidad:
Los documentos que se encuentra en esta plataforma son solo para uso interno de la institución.		

Tabla 88 Perfilamiento del activo sistema del digitalizador de documentos

Fuente: Elaboración propia

Perfilamiento del activo Documentos

Perfil de activos de información	
Activo Critico:	Documentos
Descripción: Es la información del GAD Municipal puede estar disponible fisca o virtual.	
Fecha de creación:	15/01/2019
Titular del activo: Todas las oficinas del GAD Municipal	
Contenedores para los activos de información	
Hardware: Servidor de aplicaciones, dispositivos USB, discos duros, CD, documentos en archivadores, computadores portátiles, PC.	
Requerimientos de seguridad	
Confidencialidad: Solo personal autorizado debe tener acceso a los documentos debido a que se encuentran en bienes de uso personal en la institución.	
Integridad: Los documentos se deben validar, además deben estar archivados y organizados de manera adecuada, para su fácil acceso en caso de requerirlos.	

Perfil de activos de información		
Activo Critico:	Documentos	
Disponibilidad: Los documentos deben estar disponibles cuando se realiza una solitud de revisión de los mismos.		
Valoración:		
Confidencialidad**:**	Integridad: X	Disponibilidad:
Los documentos almacenados deben estar validados y solo personas con autorización pueden realizar una modificación.		

Tabla 89 Perfilamiento del activo Documentos

Fuente: Elaboración propia

Perfilamiento del activo Directorio Activo

Perfil de activos de información		
Activo Critico:	Directorio Activo	
Descripción: Almacena datos personales de los empleados, así como los roles, usurarios y contraseñas asignadas al personal del GAD.		
Fecha de creación:	15/01/2019	
Titular del activo: Jefe de Departamento Tecnológico		
Contenedores para los activos de información		
Hardware: Servidor de aplicaciones		
Requerimientos de seguridad		
Confidencialidad: Solo el jede del departamento tecnológico, puede acceder al sistema para realizar las acciones que se requiera.		
Integridad: La información que se almacena debe ser verídica y comprobada ya que es información del personal de la entidad.		
Disponibilidad: Siempre debe estar disponible porque en ella esta los roles asignados para cada empleado.		
Valoración		
Confidencialidad:	Integridad:	Disponibilidad: X
Al menos durante la jornada laboral deberá estar disponible para que las actividades de la entidad no se vean afectadas.		

Tabla 90 Perfilamiento del activo Directorio Activo

Fuente: Elaboración propia

Perfilamiento del activo Servidor de aplicaciones

Perfil de activos de información		
Activo Critico:	Servidor de aplicaciones	
Descripción: Aloja las aplicaciones que se ejecutan el GAD municipal (Cabildo, Proxy, Squid, Antivirus, Directorio Activo, Documentos)		
Fecha de creación:	15/01/2019	
Titular del activo: jefe de departamento tecnológico, Ingeniero de redes		
Contenedores para los activos de información		
Hardware: Servidor de aplicaciones.		
Requerimientos de seguridad		
Confidencialidad: Solo el jefe de Departamento Tecnológico y el ingeniero de redes pueden ingresar u otorgar autorización para el ingreso al servidor.		
Integridad: Las aplicaciones instaladas en el servidor deben funcionar correctamente, además todos los datos almacenados deben ser verídicos.		
Disponibilidad: Debe estar disponible ya que las principales aplicaciones del GAD corren en este servidor.		
Valoración:		
Confidencialidad:	Integridad:	Disponibilidad: X
Lo ideal es que el Servidor funcione continuamente para no tener inconvenientes con las actividades cotidianas de la entidad.		

Tabla 91 Perfilamiento del activo Servidor de aplicaciones

Fuente: Elaboración propia

Perfilamiento del activo servidor de desarrollo

Perfil de activos de información	
Activo Critico:	Servidor de desarrollo.
Descripción: Se alojan los entornos de desarrollo en los que el departamento tecnológico crea nuevos módulos con el fin de mejorar los procesos de la institución.	
Fecha de creación:	15/01/2019
Titular del activo: jefe de Departamento Tecnológico, Ingeniero encargado de desarrollo	
Contenedores para los activos de información	

Perfil de activos de información		
Activo Critico:	Servidor de desarrollo.	
Hardware: Servidor de Desarrollo.		
Requerimientos de seguridad		
Confidencialidad: Solo el jefe de Departamento Tecnológico y el ingeniero de desarrollo pueden ingresar u otorgar autorización para el ingreso al servidor.		
Integridad: Los módulos y aplicaciones creadas por los desarrolladores deben estar documentadas y almacenadas en el servidor.		
Disponibilidad: El servidor debe estar disponible cuando el desarrollador lo requiera.		
Valoración		
Confidencialidad:	Integridad:	Disponibilidad: X
Debe estar disponible durante el tiempo que se está desarrollando por lo general el desarrollador del GAD utiliza 3 horas diarias, ya que tiene otras tareas asignadas.		

Tabla 92 Perfilamiento del activo servidor de desarrollo

Fuente: Elaboración propia

Perfilamiento del activo servidor de Pruebas

Perfil de activos de información	
Activo Critico:	Servidor de pruebas.
Descripción: Permite evaluar el rendimiento y funcionamiento de aplicaciones que se plantean ingresar a producción en el GAD, también ayuda a la evaluación de los módulos desarrollados por el área de sistemas.	
Fecha de creación:	15/01/2019
Titular del activo: Integrantes del Departamento Tecnológico	
Contenedores para los activos de información	
Hardware: Servidor de pruebas**.**	
Requerimientos de seguridad	
Confidencialidad: Solo el jefe de Departamento Tecnológico y el ingeniero de desarrollo pueden ingresar u otorgar autorización para el ingreso al servidor.	

Perfil de activos de información		
Activo Critico:	Servidor de pruebas.	
Integridad: Las pruebas de las aplicaciones o módulos deben ser documentadas con el fin de decidir si es factible la instalación en el servidor de aplicaciones y su posterior puesta en producción.		
Disponibilidad: El servidor debe estar disponible cuando se tiene programado realizar pruebas a los sistemas nuevos.		
Valoración:		
Confidencialidad:	Integridad: X	Disponibilidad:
La documentación verídica sobre las pruebas de la aplicaciones o módulos ayudaran a la toma de decisiones en la entidad.		

Tabla 93 Perfilamiento del activo servidor de Pruebas

Fuente: Elaboración propia

ANEXO E: Áreas de Preocupación

Análisis de las áreas de preocupación para el activo Correo electrónico

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Correo electrónico			
Motivos:	Intereses personales, robo			
Resultados:	Divulgación: X	Modificación:	Destrucción:	Interrupción:
Requisito de seguridad:	Solo los integrantes del departamento tecnológico tienen acceso al servidor de correo mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 94 Activo Correo electrónico, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El personal del departamento tecnológico es el único que tiene acceso a los servidores físicos.			

Tabla 95 Activo Correo electrónico, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	personal interno y externo			
Medio:	Ingreso al correo electrónico			
Motivos:	Intereses personales, divulgación información, falta de conocimiento			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo personal autorizado puede ingresar al servidor de correo electrónico mediante usuarios y contraseñas otorgadas por el jefe de departamento tecnológico.			

Tabla 96 Activo Correo electrónico, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Interrupción en el servicio de energía electrónica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 97 Activo Correo electrónico, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la Organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El correo electrónico no estará disponible si hay problemas en la red hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 98 Activo Correo electrónico, área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Falta de comunicación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción :X
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas			

Tabla 99 Activo Correo electrónico, área de preocupación Interrupción en el servicio internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico debe manipular y realizar revisiones de servidor en el que se encuentra el servicio de correo electrónico, en caso de presentar falla el servicio de base de datos se detendrá hasta identificar y solucionar el problema.			

Tabla 100 Activo Correo electrónico, área de preocupación Falla en los componentes de hardware en los equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de servicio de correo electrónico, pero primero se debe realizar una evaluación en el servidor de pruebas para verificar si funciona correctamente.			

Tabla 101 Activo Correo electrónico, área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos			
Resultados:	Divulgación:	Modificación:	Destrucción. X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 102 Activo Correo electrónico, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Correo electrónico			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El servicio de correo electrónico se detendrá hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 103 Activo Correo electrónico, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

Análisis de las áreas de preocupación del activo Digitalizador de documentos

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno.			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales, robo.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de Seguridad:	Para la consultar, modificar o ingresar un documento se debe acceder con el usuario y contraseña asignado por el jefe de departamento tecnológico.			

Tabla 104 Activo Digitalizador de documentos, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos.			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno y externo			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado			
Motivos:	Intereses personales, robo.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El digitalizador de documentos puede ser utilizado solo por personal autorizado y con el fin de respaldar documento s importantes.			

Tabla 105 Activo Digitalizador de documentos, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	Personal interno			
Medio:	Ingreso al sistema digitalizador de documentos			
Motivos:	Desconocimiento en el manejo del sistema. Falta de capacitación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo personal autorizado y capacitado puede manipular la digitalización de documentos.			

Tabla 106 Activo Digitalizador de documentos, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Interrupción en el servicio de energía electrónica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 107 Activo Digitalizador de documentos, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	Personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Falta de capacitación, intereses personales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La digitalización de documentos no estará disponible si hay problemas en la red hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 108 Activo Digitalizador de documentos, área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor. Falla en los dispositivos. Mantenimiento por parte del proveedor			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 109 Activo Digitalizador de documentos, área de preocupación Interrupción en el servicio internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático			
Motivos:	Falla de fabricación, mala manipulación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico debe manipular y realizar revisiones de los elementos físicos que interviene en el proceso de digitalización, en caso de presentar falla el servicio se detiene hasta encontrar el problema y corregirlo. En caso que el escáner este defectuoso se requería de terceros para la reparación o a su vez contactarse con el proveedor para la adquisición de un nuevo equipo.			

Tabla 110 Activo Digitalizador de documentos, área de preocupación Falla en los componentes de hardware en los equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El usuario no debe realizar las actualizaciones o modificaciones al sistema ese puede provocar que el escáner no sea detectado, la digitalización no estará disponible hasta que el departamento tecnológico encontré la falla y la solucionarla.			

Tabla 111 Activo Digitalizador de documentos, área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos			
Resultados:	Divulgación:	Modificación:	Destrucción: X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 112 Activo Digitalizador de documentos, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Sistema Digitalizador de Documentos			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La digitalización de documentos se detendrá hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 113 Activo Digitalizador de documentos, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

4.7.1.3 Análisis de las áreas de preocupación del activo Documentos.

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Correo electrónico, dispositivos de almacenamiento			
Motivos:	Intereses personales, robo.			
Resultados:	Divulgación: X	Modificación:	Destrucción:	Interrupción:
Requisito de seguridad:	Solo personal autorizado puede ingresar a los documentos mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 114 Activo Documentos, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno.			
Medio:	Ingreso a los documentos de otros usuarios si n autorización en la PC, Laptop u otro dispositivo de almacenamiento			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Todos los usuarios deben contar con un usuario y contraseña para resguardar la información. En el caso de dispositivos de almacenamiento portátil solo se puede utilizar con el consentimiento de la persona encargada del dispositivo.			

Tabla 115 Activo Documentos, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos.			
Actor:	Personal interno.			
Medio:	Correo electrónico, dispositivos de almacenamiento			
Motivos:	Intereses personales, desconocimiento de la aplicación.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo personal autorizado puede tener acceso a los documentos.			

Tabla 116 Activo Documentos, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos			
Área de preocupación:	Interrupción en el servicio de energía electrónica.			
Actor:	Personal interno y externo.			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Los documentos almacenados en computadoras o servidores no estarán disponibles. Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 117 Activo Documentos, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Problemas de conectividad en la red interna de la organización.			
Actor:	Personal interno.			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la Organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Los Documentos que están alojados en el servidor no estará disponible hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 118 Activo Documentos, área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Interrupción en el servicio de internet.			
Actor:	Personal externo.			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La consulta de documentos a través de la página web de la entidad no estará disponible internamente. Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 119 Activo Documentos, área de preocupación Interrupción en el servicio de internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos.			
Actor:	Personal interno.			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación, Accidental			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico debe manipular y realizar revisiones de dispositivos que ayudan a la obtención documentos (impresora, computador), en caso de presentar falla los miembros del departamento tecnológico deben proveer una solución.			

Tabla 120 Activo Documentos, área de preocupación Falla en los componentes de hardware en los equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Actualización o instalación de software sin autorización.			
Actor:	Personal interno y externo.			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El usuario no debe realizar las actualizaciones o modificaciones al sistema ese puede provocar la detención de servicios, el área de departamento tecnológico es el encargado de realizar estas acciones.			

Tabla 121 Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Desastres naturales.			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Causas naturales.			
Resultados:	Divulgación:	Modificación:	Destrucción: X	Interrupción:
Requisito de seguridad	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 122 Activo Documentos, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Documentos.			
Área de preocupación:	Fallo o defecto de software.			
Actor:	Personal interno, personal externo.			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La generación de documentos se detendrá hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 123 Activo Documentos, área de preocupación Fallo o defecto de software.

Fuente: Elaboración propia

Análisis de las áreas de preocupación del activo Intranet.

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales			
Resultados:	Divulgación: X	Modificación:	Destrucción:	Interrupción:
Requisito de seguridad:	Solo los integrantes del departamento tecnológico tienen acceso a la intranet mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico, además la persona más propensa a realizar cambios es el ingeniero encargado de redes Ing. Julio Flores.			

Tabla 124 Activo Intranet, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura informáticos.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado.			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El personal del departamento tecnológico es el único que tiene acceso a los servidores y racks de la entidad.			

Tabla 125 Activo Intranet, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Ingreso a la intranet			
Motivos:	Intereses personales, divulgación información, falta de conocimiento			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo los integrantes del departamento tecnológico tienen acceso a la intranet mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico			

Tabla 126 Activo Intranet, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Interrupción en el servicio de energía electrónica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción. X
Requisito de seguridad:	La intranet no estará en funcionamiento. Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 127 Activo Intranet, área de preocupación Interrupción en el servicio de energía electrónica

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales, Daño a la organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Únicamente el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 128 Activo Intranet, área de preocupación Problemas de conectividad en la red interna de la organización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Causas naturales			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La intranet funcionará, pero no permitirá a los usuarios la conexión a la web. La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 129 Activo Intranet, área de preocupación Interrupción en el servicio internet

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico debe manipular y realizar revisiones de la intranet, en caso de presentar falla no se tendrá conexión hasta identificar y solucionar el problema.			

Tabla 130 Activo Intranet, área de preocupación Falla en los componentes de hardware en los equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de algún servicio en la intranet, pero primero se debe realizar una evaluación en el servidor de pruebas para verificar si funciona correctamente.			

Tabla 131 Activo Intranet, área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Causas naturales			
Resultados:	Divulgación:	Modificación:	Destrucción: X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 132 Activo Intranet, área de preocupación Desastres naturales

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Intranet			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La intranet no funcionara hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 133 Activo Intranet, área de preocupación Falla o defecto de software

Fuente: Elaboración propia

Análisis en cada una de las áreas de preocupación para el activo Directorio Activo

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Ingreso a la aplicación utilizando credenciales de otros usuarios internos de la entidad			
Motivos:	Intereses personales, robo			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo el jefe de departamento tecnológico tiene acceso al directorio activo y es el único que puede añadir, crear y modificar.			

Tabla 134 Activo Directorio Activo, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Únicamente el personal del departamento tecnológico es el único que tiene acceso al data center de la institución.			

Tabla 135 Activo Directorio Activo, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos			
Actor:	personal interno y externo			
Medio:	Ingreso al Sistema			
Motivos:	Intereses personales, divulgación información, falta de conocimiento			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo el jefe de departamento tecnológico tiene acceso al directorio activo y es el único que puede añadir, crear y modificar.			

Tabla 136 Activo Directorio Activo, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Interrupción en el servicio de energía eléctrica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 137 Activo Directorio Activo, área de preocupación Interrupción en el servicio de energía electrónica

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la Organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Directorio Activo no estará disponible y por ende tampoco funcionaran las aplicaciones que están regidas por los roles que asigna el administrador, esto será hasta que se encuentre y solucione el inconveniente, únicamente el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 138 Activo Directorio Activo, área de preocupación Problemas de conectividad en la red interna de la organización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 139 Activo Directorio Activo, área de preocupación Interrupción en el servicio internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el departamento tecnológico puede realizar una revisión de los dispositivos hardware y software que puedan interrumpir las funciones del directorio activo.			

Tabla 140 Activo Directorio Activo, área de preocupación Falla en los componentes de hardware en los equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Únicamente el personal del departamento tecnológico está autorizado para realizar la actualización de algún componente del directorio activo, pero primero se debe realizar una evaluación en el servidor de pruebas para verificar si funciona correctamente.			

Tabla 141 Activo Directorio Activo, área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Desastres naturales			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos			
Resultados:	Divulgación:	Modificación:	Destrucción. X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 142 Activo Directorio Activo, área de preocupación Desastres naturales

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Directorio Activo			
Área de preocupación:	Falla o defecto de software			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El directorio activo no estará disponible hasta que se encuentre lo que produjo la falla y logre solucionarlo, esto está a cargo del área del departamento tecnológico.			

Tabla 143 Activo Directorio Activo, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

Análisis de las áreas de preocupación para el activo Servidor de aplicaciones

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno.			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales, robo.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo los integrantes del departamento tecnológico tienen acceso al servidor de aplicaciones mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 144 Activo Servidor de aplicaciones, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno.			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado.			
Motivos:	Intereses personales.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	El personal del departamento tecnológico es el único que tiene acceso al data center donde se encuentra el servidor de aplicaciones.			

Tabla 145 Activo Servidor de aplicaciones, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos.			
Actor:	Personal interno y externo.			
Medio:	Ingreso al Servidor de aplicaciones.			
Motivos:	Intereses personales, divulgación información, falta de conocimiento.			
Resultados:	Divulgación:	Modificación	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo los integrantes del departamento tecnológico tienen acceso al servidor de aplicaciones mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 146 Activo Servidor de aplicaciones, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Interrupción en el servicio de energía electrónica.			
Actor:	Agentes externos.			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 147 Activo Servidor de aplicaciones, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Problemas de conectividad en la red interna de la organización.			
Actor:	Personal interno y externo.			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la organización.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El servidor de aplicaciones estará en funcionamiento, pero no tendrá comunicación hasta que se encuentre y solucione el inconveniente, solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 148 Activo Servidor de aplicaciones, área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Interrupción en el servicio internet.			
Actor:	Agentes externos.			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 149 Activo Servidor de aplicaciones, área de preocupación Interrupción en el servicio internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos.			
Actor:	Personal interno y externo.			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Únicamente el departamento tecnológico debe manipular y realizar revisiones de servidores, en caso de presentar falla el servidor deberá parar la producción hasta identificar y solucionar el problema.			

Tabla 150 Activo Servidor de aplicaciones, área de preocupación Falla en los componentes de hardware en los equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Actualización o instalación de software sin autorización.			
Actor:	Personal interno y externo.			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de sistema o algún componente de Servidor de aplicaciones, pero primero se debe realizar una evaluación en el servidor de pruebas para verificar si el funcionamiento es correcto.			

Tabla 151 Activo Servidor de aplicaciones, área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Desastres naturales.			
Actor:	Fenómenos naturales.			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos.			
Resultados:	Divulgación:	Modificación:	Destrucción. X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 152 Activo Servidor de aplicaciones, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de aplicaciones.			
Área de preocupación:	Falla o defecto de software.			
Actor:	Personal interno o externo.			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El Servidor de Aplicaciones no prestara sus funciones hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 153 Activo Servidor de aplicaciones, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

Análisis de las áreas de preocupación para el activo Servidor de desarrollo

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales, robo			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Únicamente los integrantes del departamento tecnológico tienen acceso al servidor de desarrollo mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 154 Activo Servidor de desarrollo, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado.			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	El personal del departamento tecnológico es el único que tiene acceso al data center donde se encuentra el servidor de aplicaciones.			

Tabla 155 Activo Servidor de desarrollo, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo.			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos.			
Actor:	Personal interno y externo			
Medio:	Ingreso al Servidor de desarrollo.			
Motivos:	Intereses personales, divulgación información, falta de conocimiento.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Solo el personal encargado de recaudo y los del área de tecnología pueden ingresar al sistema, ya que son los únicos que cuentan con usuario y contraseña.			

Tabla 156 Activo Servidor de desarrollo, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo			
Área de preocupación:	Interrupción en el servicio de energía electrónica			
Actor:	Agentes externos			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 157 Activo Servidor de desarrollo, área de preocupación Interrupción en el servicio de energía electrónica

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la Organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 158 Activo Servidor de desarrollo, área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo.			
Área de preocupación:	Interrupción en el servicio internet.			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red.			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 159 Activo Servidor de desarrollo, área de preocupación Interrupción en el servicio internet.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo.			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Únicamente el departamento tecnológico debe manipular y realizar revisiones de servidores, en caso de presentar falla el servidor deberá parar la producción hasta identificar y solucionar el problema.			

Tabla 160 Activo Servidor de desarrollo, área de preocupación Falla en los componentes de hardware en los equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo.			
Área de preocupación:	Actualización o instalación de software sin autorización.			
Actor:	Personal interno y externo.			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de sistema o algún componente de Servidor de desarrollo, pero primero se debe realizar una evaluación en el servidor de pruebas para verificar si el funcionamiento es correcto.			

Tabla 161 Activo Servidor de desarrollo, área de preocupación Actualización o instalación de software sin autorización.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo.			
Área de preocupación:	Desastres naturales.			
Actor:	Fenómenos naturales.			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos.			
Resultados:	Divulgación:	Modificación:	Destrucción. X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 162 Activo Servidor de desarrollo, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de desarrollo.			
Área de preocupación:	Falla o defecto de software.			
Actor:	Personal interno o externo.			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación, falta de presupuesto.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El Servidor de desarrollo no prestara sus funciones hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 163 Activo Servidor de desarrollo, área de preocupación Falla o defecto de software.

Fuente: Elaboración propia

Análisis en de las áreas de preocupación para el activo servidor de pruebas

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Actor:	Personal interno.			
Medio:	Ingresando al activo de información utilizando la clave de un usuario con privilegios.			
Motivos:	Intereses personales			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	Únicamente los integrantes del departamento tecnológico tienen acceso al servidor de pruebas mediante usuarios y contraseñas asignados por el jefe de departamento tecnológico.			

Tabla 164 Activo Servidor de pruebas, área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Exposición de los activos de información, acceso no autorizado a la infraestructura física.			
Actor:	Personal interno.			
Medio:	Ingreso al data center o a las oficinas sin ser autorizado.			
Motivos:	Intereses personales.			
Resultados:	Divulgación:	Modificación: X	Destrucción:	Interrupción:
Requisito de seguridad:	El personal del departamento tecnológico es el único que tiene acceso al data center.			

Tabla 165 Activo Servidor de pruebas, área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas.			
Área de preocupación:	Desconocimiento en el manejo de los sistemas o equipos informáticos.			
Actor:	Personal interno y externo.			
Medio:	Ingreso al Sistema.			
Motivos:	Intereses personales, divulgación información, falta de conocimiento.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo personal autorizado puede ingresar a la base de datos mediante usuarios y contraseñas otorgadas por el jefe de departamento tecnológico.			

Tabla 166 Activo Servidor de pruebas, área de preocupación Desconocimiento en el manejo de los sistemas o equipos informáticos.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas.			
Área de preocupación:	Interrupción en el servicio de energía electrónica.			
Actor:	Agentes externos.			
Medio:	Descarga eléctrica Falta de pago al proveedor Falla de los equipos alternos			
Motivos:	Causas naturales Sobre carga de energía. Falta de Mantenimiento			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Se debe contar con un generador eléctrico que suministre energía a los equipos y restablecer el servicio o al menos contar con equipos UPS para evitar el daño de equipos.			

Tabla 167 Activo Servidor de pruebas, área de preocupación Interrupción en el servicio de energía electrónica.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Problemas de conectividad en la red interna de la organización			
Actor:	personal interno y externo			
Medio:	Manipulación de los dispositivos de red, falta de capacitación, saturación del canal de comunicación, configuración errónea de los dispositivos de comunicación			
Motivos:	Intereses personales Daño a la organización			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico puede manipular los dispositivos de la red interna.			

Tabla 168 Activo Servidor de pruebas, área de preocupación Problemas de conectividad en la red interna de la organización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Interrupción en el servicio internet			
Actor:	Agentes externos			
Medio:	Falta de pago al proveedor El proveedor del servicio de internet realiza mantenimiento de equipos de red			
Motivos:	Accidental Falta de comunicación entre proveedor y cliente.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.			

Tabla 169 Activo Servidor de pruebas, área de preocupación Interrupción en el servicio internet

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Falla en los componentes de hardware en los equipos informáticos			
Actor:	Personal interno y externo			
Medio:	Manipulación en los equipos informáticos Conexión errónea de equipos informáticos. Uso inadecuado de los equipos informáticos. Falta de protección en las variaciones de voltaje. Falta de monitoreo de los componentes del equipo informático.			
Motivos:	Falta de capacitación, Accidental, falla de fabricación.			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Únicamente el departamento tecnológico debe manipular y realizar revisiones de servidores, en caso de presentar falla el servidor deberá parar la producción hasta identificar y solucionar el problema.			

Tabla 170 Activo Servidor de pruebas, área de preocupación Falla en los componentes de hardware en los equipos informáticos

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas			
Área de preocupación:	Actualización o instalación de software sin autorización			
Actor:	Personal interno y externo			
Medio:	El personal actualiza o instala software			
Motivos:	Falta de conocimiento, intereses propios			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Solo el personal del departamento tecnológico está autorizado para realizar la actualización de sistema.			

Tabla 171 Activo Servidor de pruebas, área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas.			
Área de preocupación:	Desastres naturales.			
Actor:	Fenómenos naturales			
Medio:	Incendios, inundaciones, tormentas eléctricas, terremotos, erupciones volcánicas			
Motivos:	Factores climáticos			
Resultados:	Divulgación:	Modificación:	Destrucción. X	Interrupción:
Requisito de seguridad:	Toda actividad del municipio se detendrá mientras se presente un desastre natural.			

Tabla 172 Activo Servidor de pruebas, área de preocupación Desastres naturales.

Fuente: Elaboración propia

Áreas de preocupación de activos de información				
Activo Critico:	Servidor de pruebas.			
Área de preocupación:	Falla o defecto de software.			
Actor:	Personal interno o externo			
Medio:	Instalación de software no licenciado. Instalación de software no compatible. Incompatibilidad con el sistema operativo Eliminación o corrupción de los archivos de instalación			
Motivos:	Falta de capacitación			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	El Servidor de Aplicaciones no prestara sus funciones hasta encontrar lo que produjo el fallo y se logre corregir, esto está a cargo del área del departamento tecnológico.			

Tabla 173 Activo Servidor de pruebas, área de preocupación Falla o defecto de software

Fuente: Elaboración propia

ANEXO F: Escenarios De Amenaza

Escenarios de amenaza del activo Correo Electrónico

Activo de Información: Correo Electrónico		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Divulgación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos.	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas.	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 174 Escenarios de amenaza del activo Correo Electrónico

Fuente: Elaboración propia

Escenarios de amenaza del activo Digitalizador de Documentos

Activo de Información: Digitalizador de Documentos		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Interrupción
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos.	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas.	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 175 Escenarios de amenaza del activo Digitalizador de Documentos

Fuente: Elaboración propia

Escenarios de amenaza del activo Documentos

Activo de Información: Documentos		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Divulgación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos.	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas.	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 176 Escenarios de amenaza del activo Documentos

Fuente: Elaboración propia

Escenarios de amenaza del activo Intranet

Activo de Información: Intranet		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Divulgación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización.	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 177 Escenarios de amenaza del activo Intranet

Fuente: Elaboración propia

Escenarios de amenaza del activo Directorio Activo

Activo de Información: Directorio Activo		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Modificación
Problemas técnicos.	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas.	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 178 Escenarios de amenaza del activo Directorio Activo

Fuente: Elaboración propia

Escenarios de amenaza del activo Servidos de Aplicaciones

Activo de Información: Servidor de Aplicaciones		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Modificación
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 179 Escenarios de amenaza del activo Servidos de Aplicaciones

Fuente: Elaboración propia

Escenarios de amenaza del activo Servidos de Desarrollo

Activo de Información: Servidor de desarrollo		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Interrupción
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 180 Escenarios de amenaza del activo Servidos de Desarrollo

Fuente: Elaboración propia

Escenarios de amenaza del activo Servidos de Pruebas

Activo de Información: Servidor de pruebas		
Árbol de amenaza	**Área de preocupación**	**Resultado**
Actores Humanos utilizando medios técnicos.	Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Modificación
	Desconocimiento en el manejo de los sistemas o equipos informáticos	Modificación
Actores Humanos utilizando medios físicos.	Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Modificación
Problemas técnicos	Problemas de conectividad en la red interna de la organización.	Interrupción
	Interrupción en el servicio de internet	Interrupción
	Falla en los componentes de hardware de los equipos	Interrupción
	Actualización o instalación de software sin autorización	Interrupción
	Fallo o defecto de Software	Interrupción
Otros Problemas	Interrupción en el servicio de energía eléctrica.	Interrupción
	Desastres Naturales	Destrucción

Tabla 181 Escenarios de amenaza del activo Servidos de Pruebas

Fuente: Elaboración propia

ANEXO G: Identificación de Riesgos

Consecuencias del correo electrónico

Activo de Información: Correo electrónico	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	-Los integrantes del departamento tecnológico deberán verificar si se realizaron modificaciones en el servicio de correo electrónico y si se encuentra información que no concuerda dicha información será eliminada de la base de datos.
Desconocimiento en el manejo de los sistemas informáticos	-Los empleados tendrán dificultad para el envió de archivos o documentos por este medio retrasando sus actividades en la institución.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-El servicio de correo electrónico estará temporalmente inhabilitado hasta que se verifique si se realizó alguna modificación o se alteró algún elemento del servidor donde está alojado.
Problemas de conectividad en la red interna de la organización	-El servicio de correo electrónico dejara de funcionar hasta que se solucione el problema de la red, provocando que la entrega de algunas solicitudes o informes de la institución se la realice físicamente para su posterior digitalización, retrasando actividades de la institución.
Interrupción en el servicio de internet	-El correo seguirá funcionando en la intranet de la institución, pero no se podrán enviar documentos que se encuentren en la web.
Falla en los componentes de hardware de los equipos	El servicio de correo electrónico estará inhabilitado hasta que los encargados identifiquen y reparen el fallo, provocando que la entrega de algunas solicitudes o informes de la institución se la realice físicamente para su posterior digitalización, retrasando actividades de la institución.
Actualización o instalación de software sin autorización	- El servicio de correo electrónico puede presentar incompatibilidad con la actualización realizada y presentar fallos.

Activo de Información: Correo electrónico	
Escenario de amenaza	**Consecuencia**
Fallo o defecto de Software	- El servicio de correo electrónico estará inhabilitado hasta solucionar el problema, provocando que la entrega de algunas solicitudes o informes de la institución se la realice físicamente para su posterior digitalización, retrasando actividades de la institución.
Interrupción en el servicio de energía eléctrica	- El servicio de correo electrónico estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	- El servicio de correo electrónico no estará disponible si un desastre natural ocurre.

Tabla 182 Consecuencias del correo electrónico

Fuente: Elaboración propia

Consecuencias del digitalizador de documentos

Activo de Información: Digitalizador de documentos	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	-Los integrantes del departamento tecnológico deben verificar si existieron modificaciones en base de documentos digitalizados durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenían planificadas. -En caso de encontrar documentos nuevos que no tenga validez o coherencia deberán ser eliminados.
Desconocimiento en el manejo de los sistemas informáticos	-Los empleados de distintas áreas del municipio tendrán dificultad para digitalizar documentos retrasando sus actividades, además solicitarán asistencia al departamento tecnológico quienes deberán dirigirse a el área de trabajo solicitada dejando de lado actividades que estaba realizando.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-El digitalizador de documentos no estará disponible hasta realizar una revisión por parte del departamento de tecnología.

Activo de Información: Digitalizador de documentos	
Escenario de amenaza	**Consecuencia**
Problemas de conectividad en la red interna de la organización	-No se podrá digitalizar documentos ya que no habrá conexión con el servidor donde se realiza el almacenamiento. -Los documentos se acumularán para su posterior digitalización.
Interrupción en el servicio de internet	-El digitalizador de documentos seguirá funcionando debido a que funciona internamente por medio de la intranet de la institución.
Falla en los componentes de hardware de los equipos	-La digitalización no se podrá realizar, hasta que se revise, repare o remplace el escáner o dispositivo que presente el daño, este significará un retraso en la actividad es de la oficina afectada.
Actualización o instalación de software sin autorización	-Los drives de los dispositivos pueden presentar incompatibilidad con la actualización, haciendo que no se pueda reconocer el escáner y por lo tanto no se pueda digitalizar.
Fallo o defecto de Software	- La digitalización estará inactiva hasta que el personal de tecnologías revise y repare el problema, los documentos a digitalizar se acumularan para realizar el proceso posteriormente.
Interrupción en el servicio de energía eléctrica	-La digitalización de documentos estará inhabilitada hasta restablecer la energía eléctrica. - Los documentos a digitalizar se acumularán para realizar el proceso posteriormente.
Desastres Naturales	-La digitalización de documentos no estará disponible si un desastre natural ocurre.

Tabla 183 Consecuencias del digitalizador de documentos

Fuente: Elaboración propia

Consecuencias del para el activo documentos

Activo de Información: Documentos	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	- La información de documentos digitales del municipio puede ser exhibidos o utilizados con fines de dañar la institución.
Desconocimiento en el manejo de los sistemas informáticos	-Los empleados tienen dificultad para ingresar al servidor donde están almacenados los documentos, retrasando sus actividades.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-La información de documentos físicos del municipio puede ser exhibidos o utilizados con fines de dañar la institución.
Problemas de conectividad en la red interna de la organización	-Las consultas de documentos almacenados en el servidor no estarán disponibles ya se todo se comunica mediante la intranet.
Interrupción en el servicio de internet	-Los documentos digitales y físicos estarán disponibles ya que todos están dentro de las instalaciones del municipio, lo que se vería afectado es la descarga de documentos que están en línea.
Falla en los componentes de hardware de los equipos	-En el caso que el fallo se produce en el servidor donde están almacenados los documentos no se tendrá acceso hasta que los encardados del departamento tecnológico solucionen el inconveniente. -Si se produce el daño de hardware (impresora, PC, laptop) en la oficina que se esta realizando la consulta, solicitan asistencia a el departamento tecnológico para que se realice las revisiones a los dispositivos. En los dos casos se producirá un atraso de actividades tanto para los encargados de tecnología como quienes trataban de realizar la consulta.

Activo de Información: Documentos	
Escenario de amenaza	**Consecuencia**
Actualización o instalación de software sin autorización	-La actualización del sistema podría hacer que no los drivers dejen de ser compatibles y no reconocer los dispositivos.
Fallo o defecto de Software	-En el caso que el fallo se produce en el servidor donde están almacenados los documentos no se tendrá acceso hasta que los encargados del departamento tecnológico solucionen el inconveniente. -Si el fallo de sistema se produce en el área que se esta consultado se debe requerir asistencia de departamento de tecnología lo que retrasara las actividades de las dos partes.
Interrupción en el servicio de energía eléctrica	- Los documentos digitales no estarán disponibles hasta restablecer la energía eléctrica.
Desastres Naturales	- Los documentos no estarán disponible si un desastre natural ocurre.

Tabla 184 Consecuencias de documentos

Fuente: Elaboración propia

Consecuencias de la Intranet

Activo de Información: Intranet	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	-El ingeniero encargado de redes debe verificar si existieron modificaciones en la intranet durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenía planificadas. -En el caso de encontrar alguna alteración se realizará un restablecimiento de una copia de seguridad de la configuración y si no se dispone tendrá que volver a configurar todos los equipos.
Desconocimiento en el manejo de los sistemas informáticos	-Los empleados se quedarían sin conexión a la red interna por distintos (modificación, eliminación de dirección asignada)**,** lo que retrasara las actividades que tiene que realizar
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	- La intranet seguirá funcionando, pero el ingeniero encargado de redes tiene que revisar si se realizó alguna modificación o se alteró el algún elemento, de ser el caso deberá solucionar el inconveniente.

Activo de Información: Intranet	
Escenario de amenaza	**Consecuencia**
Problemas de conectividad en la red interna de la organización	-La intranet estará inhabilitada hasta identificar y reparar el problema, las actividades del municipio se verán afectadas.
Interrupción en el servicio de internet	- La intranet seguirá disponible, pero para consultas de la página web estará fuera de servicio mientras se restablece la conectividad a internet.
Falla en los componentes de hardware de los equipos	-Los empleados que estén conectados al dispositivo (switch, router) afectado, no podrán tener acceso a los sistemas, ni a internet hasta que se repare o remplace el terminal
Actualización o instalación de software sin autorización	-La intranet puede presentar incompatibilidad con la actualización realizada y presentar fallos.
Fallo o defecto de Software	- El municipio no tendrá conexión en ciertas áreas, el ingeniero encargado de redes deberá identificar y solucionar el inconveniente.
Interrupción en el servicio de energía eléctrica	- La intranet estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	- La intranet estará disponible si un desastre natural ocurre.

Tabla 185 Consecuencias la Intranet

Fuente: Elaboración propia

Consecuencias del Directorio Activo

Activo de Información: Directorio Activo	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	-El municipio detiene las actividades de las áreas que utilicen sistemas, ya que la información que hay en el directorio activo es confidencial ya que así se asignan roles, el jefe de departamento tecnológico deberá realizar el trabajo de verificar los roles asignados a cada empleado y estableces nuevas contraseñas.
Desconocimiento en el manejo de los sistemas informáticos	-En caso de no estar el jefe del departamento de tecnología, toma el cargo el ingeniero de redes, pero a él no se le puede solicitar cambio de contraseñas o modificación de los datos que esta en el directorio activo por lo que quien solicite necesariamente tendrá que esperar la presencia del jefe.

Activo de Información: Directorio Activo	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-El directorio activo estará temporalmente inhabilitado y por ende las aplicaciones a las que esta asignados los usuarios y contraseñas, hasta que el jefe de departamento tecnológico verifique si se realizó alguna modificación o se alteró algún elemento del servidor donde está alojado.
Problemas de conectividad en la red interna de la organización	- El directorio activo y todas las aplicaciones que este asigna permisos estarán suspendidas temporalmente hasta que se restablezca la conectividad generando retrasos y pérdidas para la institución.
Interrupción en el servicio de internet	-El directorio activo funcionara sin inconvenientes en la institución.
Falla en los componentes de hardware de los equipos	-El directorio activo estará inhabilitado hasta que el departamento tecnológico encuentre y solucione lo que produjo el problema.
Actualización o instalación de software sin autorización	- El directorio activo puede presentar incompatibilidad con la actualización y puede dejar de funcionar.
Fallo o defecto de Software	- El directorio activo estará temporalmente inhabilitado y por ende las aplicaciones a las que esta asignados los usuarios y contraseñas, hasta que el jefe de departamento tecnológico solucione la falla.
Interrupción en el servicio de energía eléctrica	-La plataforma de pago no estará disponible hasta restablecer la energía eléctrica
Desastres Naturales	- El directorio activo no estará disponible si un desastre natural ocurre

Tabla 186 Consecuencias del Directorio Activo

Fuente: Elaboración propia

Consecuencias del Servidor de Aplicaciones

Activo de Información: Servidor de Aplicaciones	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	- Los integrantes del departamento tecnológico deben verificar si existieron modificaciones en el servidor de aplicaciones durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenían planificadas. -Si se encuentran modificaciones en las aplicaciones o configuraciones se detendrá momentáneamente las actividades de servidor y se tendrá que restablecer con una copia de seguridad.
Desconocimiento en el manejo de los sistemas informáticos	-En el caso que no se tenga conocimientos de un sistema se solicitara la contratación de terceros teniendo en cuenta que la información de la institución estaría expuesta.
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	- El servidor de aplicaciones y por ende los sistemas que este contiene no estarán habilitados hasta verificar si se modificó o altero algún elemento.
Problemas de conectividad en la red interna de la organización	El servidor de aplicaciones estará disponible pero no tendrá comunicación, por lo tanto, se suspenderán los servicios del municipio generando retrasos y pérdidas para la institución.
Interrupción en el servicio de internet	-El servidor estará disponible, pero en caso que las aplicaciones instaladas requieran de este internet no funcionará y se detendrá las actividades en ciertas áreas.
Falla en los componentes de hardware de los equipos	-El servidor de aplicaciones no estará disponible hasta que los encargados identifiquen y reparen el fallo, por lo que las actividades de las áreas que utilicen los sistemas instalados en este servidor verán interrumpidas sus actividades, generado pérdidas y retrasos en la institución.

Activo de Información: Servidor de Aplicaciones	
Escenario de amenaza	**Consecuencia**
Actualización o instalación de software sin autorización	-El servidor de aplicaciones puede presentar incompatibilidad con la actualización instalada y presentar fallos que podrían detener las actividades del municipio.
Fallo o defecto de Software	- Las actividades de las áreas que utilizan sistemas instalados en este servidor tienen que detenerse hasta que el departamento tecnológico solucione el problema.
Interrupción en el servicio de energía eléctrica	-El servidor de aplicaciones estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	El servidor de aplicaciones no estará disponible si un desastre natural ocurre.

Tabla 187 Consecuencias del Servidor de Aplicaciones

Fuente: Elaboración propia

Consecuencias del Servidor de Desarrollo

Activo de Información: Servidor de Desarrollo	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	-El ingeniero encargado de desarrollo debe verificar si existieron modificaciones en el servidor durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenían planificadas. - Si se encuentran modificaciones en las aplicaciones o configuraciones se detendrá momentáneamente las actividades de servidor y se tendrá que restablecer con una copia de seguridad.
Desconocimiento en el manejo de los sistemas informáticos	-El encargado de desarrollo deberá investigar por cuenta propia y resolver la duda.

Activo de Información: Servidor de Desarrollo	
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	El servidor de desarrollo no estará habilitado hasta verificar si se modificó o altero algún elemento.
Problemas de conectividad en la red interna de la organización	-El servidor de desarrollo estará disponible pero no tendrá comunicación con los elementos de la red.
Interrupción en el servicio de internet	- El servidor estará disponible, pero no podrá tener acceso a web service.
Falla en los componentes de hardware de los equipos	-El servidor de desarrollo no estará disponible hasta que los encargados identifiquen y reparen el fallo, pueden afectar las actividades planeadas del desarrollador.
Actualización o instalación de software sin autorización	-El servidor de desarrollo puede presentar incompatibilidad con la actualización instalada y presentar fallos en la comunicación o a su vez en los entornos de desarrollo.
Fallo o defecto de Software	-El ingeniero encargado de desarrollo detendrá sus actividades y deberá identificar la falla y solucionarlo.
Interrupción en el servicio de energía eléctrica	-El servidor de desarrollo estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	- El servidor de aplicaciones no estará disponible si un desastre natural ocurre.

Tabla 188 Consecuencias del Servidor de Desarrollo

Fuente: Elaboración propia

Consecuencias del Servidor de Pruebas

Activo de Información: Servidor de Pruebas	
Escenario de amenaza	**Consecuencia**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos	- Los integrantes del departamento tecnológico deben verificar si existieron modificaciones en el servidor de pruebas durante el tiempo de exposición, esto quitara el tiempo para las actividades que tenían planificadas. -Si se encuentran modificaciones en las aplicaciones o configuraciones se detendrá momentáneamente las actividades de servidor y se tendrá que restablecer con una copia de seguridad.
Desconocimiento en el manejo de los sistemas informáticos	-No se verá afectado ya que este servidor sirve para evaluar los sistemas
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	-El servidor de pruebas no estará habilitado hasta verificar si se modificó o altero algún elemento.
Problemas de conectividad en la red interna de la organización	- El servidor de pruebas estará disponible pero no tendrá comunicación con red, pero no afectará en las actividades de la institución.
Interrupción en el servicio de internet	- El servidor estará disponible, pero en caso que las aplicaciones instaladas requieran de este internet no funcionaran, sin afectar la institución.
Falla en los componentes de hardware de los equipos	-El servidor de pruebas no estará disponible hasta que los encargados identifiquen y reparen el fallo.
Actualización o instalación de software sin autorización	-No se verá afectado ya que este servidor sirve para evaluar los sistemas nuevos.

Activo de Información: Servidor de Pruebas	
Escenario de amenaza	**Consecuencia**
Fallo o defecto de Software	-Los integrantes del departamento tecnológico verificaran que sistemas producen error y crearan un informe para que no se pongan en producción.
Interrupción en el servicio de energía eléctrica	- El servidor de pruebas estará inhabilitada hasta restablecer la energía eléctrica.
Desastres Naturales	- El servidor de pruebas no estará disponible si un desastre natural ocurre.

Tabla 189 Consecuencias del Servidor de Pruebas

Fuente: Elaboración propia

ANEXO H: Análisis de Riesgos

Análisis de riesgos del Correo Electrónico

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 190 Análisis de riesgos del Correo electrónico en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 191 Análisis de riesgos del Correo electrónico en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 192 Análisis de riesgos del Correo electrónico en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 193 Análisis de riesgos del Correo electrónico en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 194 Análisis de riesgos del Correo electrónico en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 195 Análisis de riesgos del Correo electrónico en el área de preocupación Falla en los componentes de hardware de los equipos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 196 Análisis de riesgos del Correo electrónico en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 197 Análisis de riesgos del Correo electrónico en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Medio (2)	8
	Legal	3	Medio (2)	6
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			32

Tabla 198 Análisis de riesgos del Correo electrónico en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			36

Tabla 199 Análisis de riesgos del Correo electrónico en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Correo Electrónico		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Medio	19
Desconocimiento en el manejo de los sistemas informáticos.	Bajo	15
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	23
Problemas de conectividad en la red interna de la organización.	Medio	23
Interrupción en el servicio de internet	Medio	28
Falla en los componentes de hardware de los equipos	Medio	19
Actualización o instalación de software sin autorización	Medio	19
Fallo o defecto de Software	Medio	24
Interrupción en el servicio de energía eléctrica.	Alto	32
Desastres Naturales	Alto	36

Tabla 200Resumen de las áreas de preocupación del activo Correo Electrónico

Fuente: Elaboración propia

Análisis de riesgos del Digitalizador de Documentos

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 201 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 202 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física**.**	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 203 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Exposición de los activos de información, acceso no autorizado.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 204 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Problemas de conectividad en la red interna de la organización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 205 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 206 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Falla en los componentes de hardware de los equipos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 207 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 208 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 209 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Interrupción en el servicio de energía eléctrica.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	3
	Total:			33

Tabla 210 Análisis de riesgos del Digitalizador de Documentos en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Digitalizador de Documentos		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Medio	19
Desconocimiento en el manejo de los sistemas informáticos.	Medio	24
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	19
Problemas de conectividad en la red interna de la organización.	Medio	24
Interrupción en el servicio de internet	Medio	24
Falla en los componentes de hardware de los equipos	Medio	23
Actualización o instalación de software sin autorización	Medio	19
Fallo o defecto de Software	Medio	24
Interrupción en el servicio de energía eléctrica.	Medio	23
Desastres Naturales	Alto	33

Tabla 211 Resumen de las áreas de preocupación del activo Digitalizador de Documentos

Fuente: Elaboración propia

Análisis de riesgos de Documentos

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 212 Análisis de riesgos de Documentos en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 213 Análisis de riesgos de Documentos en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 214 Análisis de riesgos de Documentos en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 215 Análisis de riesgos de Documentos en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 216 Análisis de riesgos de Documentos en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos	Financiera	5	Bajo (1)	5
	Productividad	4	Alta (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 217 Análisis de riesgos de Documentos en el área de preocupación Falla en los componentes de hardware de los equipos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 218 Análisis de riesgos de Documentos en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 219 Análisis de riesgos de Documentos en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (2)	6
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 220 Análisis de riesgos de Documentos en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 221 Análisis de riesgos de Documentos en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Documentos		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Medio	24
Desconocimiento en el manejo de los sistemas informáticos.	Bajo	15
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	24
Problemas de conectividad en la red interna de la organización.	Medio	28
Interrupción en el servicio de internet	Medio	28
Falla en los componentes de hardware de los equipos	Medo	23
Actualización o instalación de software sin autorización	Medio	24
Fallo o defecto de Software	Medio	19
Interrupción en el servicio de energía eléctrica.	Medio	24
Desastres Naturales	Alto	33

Tabla 222 Resumen de las áreas de preocupación del activo Documentos

Fuente: Elaboración propia

Análisis de riesgos de Intranet

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Bajo (1)	4
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			25

Tabla 223 Análisis de riesgos de la Intranet en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 224 Análisis de riesgos de la Intranet en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (1)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 225 Análisis de riesgos de la Intranet en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 226 Análisis de riesgos de la Intranet en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 227 Análisis de riesgos de la Intranet en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 228 Análisis de riesgos de la Intranet en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 229 Análisis de riesgos de la Intranet en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Rankin g	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 230 Análisis de riesgos de la Intranet en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 231 Análisis de riesgos de la Intranet en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Medio (2)	2
	Total:			24

Tabla 232 Análisis de riesgos de la Intranet en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Intranet		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no torizado a los sistemas informáticos.	Medio	25
Desconocimiento en el manejo de los sistemas informáticos.	Bajo	15
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	24
Problemas de conectividad en la red interna de la organización.	Medio	28
Interrupción en el servicio de internet	Medio	28
Falla en los componentes de hardware de los equipos	Medio	19
Actualización o instalación de software sin autorización	Medio	19
Fallo o defecto de Software	Medio	19
Interrupción en el servicio de energía eléctrica.	Medio	23
Desastres Naturales	Medio	24

Tabla 233 Resumen de las áreas de preocupación del activo Intranet

Fuente: Elaboración propia

Análisis de riesgos de Directorio Activo

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 234 Análisis de riesgos del Directorio Activo en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 235 Análisis de riesgos del Directorio Activo en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 236 Análisis de riesgos del Directorio Activo en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 237 Análisis de riesgos del Directorio Activo en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 238 Análisis de riesgos del Directorio Activo en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 239 Análisis de riesgos del Directorio Activo en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 240 Análisis de riesgos del Directorio Activo en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Área de impacto	Rankin g	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 241 Análisis de riesgos del Directorio Activo en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 242 Análisis de riesgos del Directorio Activo en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 243 Análisis de riesgos del Directorio Activo en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Directorio Activo		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no torizado a los sistemas informáticos.	Medio	19
Desconocimiento en el manejo de los sistemas informáticos.	Medio	19
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	24
Problemas de conectividad en la red interna de la organización.	Alto	33
Interrupción en el servicio de internet	Alto	28
Falla en los componentes de hardware de los equipos	Medio	24
Actualización o instalación de software sin autorización	Medio	24
Fallo o defecto de Software	Medio	24
Interrupción en el servicio de energía eléctrica.	Alto	33
Desastres Naturales	Medio	24

Tabla 244 Resumen de las áreas de preocupación del activo Directorio Activo

Fuente: Elaboración propia

Análisis de riesgos de Servidor de Aplicaciones

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 245 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 246 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 247 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 248 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 249 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 250 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 251 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Rankin g	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Medio (2)	10
	Productividad	4	Alto (2)	12
	Legal	3	Alto (3)	9
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			36

Tabla 252 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (2)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (2)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 253 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Medio (2)	4
	Seguridad /Salud	1	Alto (3)	3
	Total:			40

Tabla 254 Análisis de riesgos del Servidor de Aplicaciones en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Servidor de Aplicaciones		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no torizado a los sistemas informáticos.	Alto	33
Desconocimiento en el manejo de los sistemas informáticos.	Medio	24
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	24
Problemas de conectividad en la red interna de la organización.	Alto	33
Interrupción en el servicio de internet	Alto	33
Falla en los componentes de hardware de los equipos	Medio	24
Actualización o instalación de software sin autorización	Medio	19
Fallo o defecto de Software	Alto	36
Interrupción en el servicio de energía eléctrica.	Alto	33
Desastres Naturales	Alto	40

Tabla 255 Resumen de las áreas de preocupación del activo Servidor de Aplicaciones

Fuente: Elaboración propia

Análisis de riesgos de Servidor de Desarrollo

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 256 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 257 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Medio (2)	10
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			28

Tabla 258 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 259 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Medio (2)	10
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			24

Tabla 260 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 261 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	1
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 262 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Bajo (1)	5
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			23

Tabla 263 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			33

Tabla 264 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Interrupción en el servicio de energía eléctrica.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Alto (3)	15
	Productividad	4	Alto (3)	12
	Legal	3	Medio (2)	6
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Medio (2)	2
	Total:			37

Tabla 265 Análisis de riesgos del Servidor de Desarrollo en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Servidor de Desarrollo		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no torizado a los sistemas informáticos.	Medio	28
Desconocimiento en el manejo de los sistemas informáticos.	Medio	24
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	28
Problemas de conectividad en la red interna de la organización.	Medio	24
Interrupción en el servicio de internet	Medio	24
Falla en los componentes de hardware de los equipos	Medio	19
Actualización o instalación de software sin autorización	Bajo	15
Fallo o defecto de Software	Medio	23
Interrupción en el servicio de energía eléctrica.	Alto	33
Desastres Naturales	Alto	37

Tabla 266 Resumen de las áreas de preocupación del activo Servidor de Desarrollo

Fuente: Elaboración propia

Análisis de riesgos de Servidor de Pruebas

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 267 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desconocimiento en el manejo de los sistemas informáticos.	Financiera	5	Bajo (1)	5
	Reputación	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Productividad	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 268 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Desconocimiento en el manejo de los sistemas informáticos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 269 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Exposición de los activos de información, acceso no autorizado a la infraestructura física.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Problemas de conectividad en la red interna de la organización.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 270 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Problemas de conectividad en la red interna de la organización.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de internet	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 271 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Interrupción en el servicio de internet

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Falla en los componentes de hardware de los equipos.	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 272 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Falla en los componentes de hardware de los equipos.

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Actualización o instalación de software sin autorización	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 273 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Actualización o instalación de software sin autorización

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Rankin g	Valor del impacto	Puntuación
Fallo o defecto de Software	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 274 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Fallo o defecto de Software

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Interrupción en el servicio de energía eléctrica.	Financiera	5	Bajo (1)	5
	Productividad	4	Medio (2)	8
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	4
	Seguridad /Salud	1	Bajo (1)	1
	Total:			19

Tabla 275 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Interrupción en el servicio de energía eléctrica

Fuente: Elaboración propia

Área de preocupación	Criterio de evaluación	Prioridad	Valor del impacto	Puntuación
Desastres Naturales	Financiera	5	Bajo (1)	5
	Productividad	4	Bajo (1)	4
	Legal	3	Bajo (1)	3
	Reputación	2	Bajo (1)	2
	Seguridad /Salud	1	Bajo (1)	1
	Total:			15

Tabla 276 Análisis de riesgos del Servidor de Pruebas en el área de preocupación Desastres Naturales

Fuente: Elaboración propia

Resumen de áreas de Preocupación del activo Servidor de Pruebas		
Área de preocupación	**Impacto**	**Puntaje**
Exposición de los activos de información, acceso no torizado a los sistemas informáticos.	Bajo	15
Desconocimiento en el manejo de los sistemas informáticos.	Medio	19
Exposición de los activos de información, acceso no autorizado a la infraestructura física.	Medio	19
Problemas de conectividad en la red interna de la organización.	Bajo	15
Interrupción en el servicio de internet	Medio	19
Falla en los componentes de hardware de los equipos	Bajo	15
Actualización o instalación de software sin autorización	Bajo	15
Fallo o defecto de Software	Medio	19
Interrupción en el servicio de energía eléctrica.	Medio	19
Desastres Naturales	Bajo	15

Tabla 277 Resumen de las áreas de preocupación del activo Servidor de Pruebas

Fuente: Elaboración propia

ANEXO I: Enfoque de mitigación

Mitigación de riesgo del activo Correo electrónico

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Correo electrónico</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
El usuario y contraseña son de uso personal no se deben exponer.
La contraseña debe ser cambiada mensualmente.</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 15</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 4</td><td>Acción:
Aceptar</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 23</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
El jefe del departamento y encargado redes puede realizar modificaciones al servidor de correo electrónico.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna.
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Correo electrónico</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos a los servidores.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente, procesador. Memoria RAM, disco duro, cables</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico puede instalar y actualizar un componente del correo electrónico.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos preventivos en los equipos que utilizan la plataforma de recaudación.
Realizar actualizaciones del sistema previo análisis en el servidor de pruebas.
Deshabilitar los servicios del ordenador que no sean necesarios.
Planificar configuración de Servidores
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
</table>

Nombre del activo:	Correo electrónico		
Área de preocupación: Interrupción en el servicio de energía eléctrica.			
Puntaje de riesgo relativo: 32	**Probabilidad subjetiva:** Alto	**Categoría:** Grupo 1	**Acción:** Mitigar
Control: • Adquirir un UPS exclusivo para el servidor de aplicaciones y así evitar daños, ya que en este se aloja los servicios necesarios para el servicio de correo electrónico. • Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.			
Área de preocupación: Desastres Naturales			
Puntaje de riesgo relativo: 36	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Realizar respaldo de información de los datos del servicio de correo electrónico y almacenarlos en la nube. • Crear un plan estratégico en caso de desastres naturales. • Mejorar la señalización en las oficinas. • Tener equipos en contra de incendios ubicados en lugares estratégicos.			

Tabla 278 Mitigación de riesgo del activo Correo electrónico
Fuente: Elaboración propia

Mitigación de riesgo del activo Digitalizador de Documentos

Nombre del activo:	Digitalizador de documentos		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 19	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control: • Solo el jefe de departamento tecnológico debe tener acceso a la administración de los documentos digitalizados. • Los usuarios de distintas áreas del municipio solo pueden digitalizar documento s por medio de un usuario y contraseña asignado por el jefe de departamento tecnológico. • Realizar diariamente copias de seguridad de los documentos digitalizados. • Realizar un log que almacene el historial de documentos digitalizados subidos al servidor en los que conste usuario, fecha, hora, nombre del documento.			

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Digitalizador de documentos</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar capacitaciones a los usuarios del correcto uso del escáner y como se subir el documento al sistema.
Realizar un manual que asista a los usuarios en caso de tener dificultas en la digitalización de documentos.</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo:19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo personal autorizado de cada oficina debe dar uso a la digitalización de documentos (escáner, sistema de digitalización).
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center y verificar los documentos.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo:24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna.
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Digitalizador de documentos</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 23</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos a los equipos.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente, procesador. Memoria RAM, disco duro, cables, escáner)</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo el personal de departamento tecnológico puede instalar y actualizar software.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.
Se debe comunicar a los empleados que no pueden instalar ningún software.
El departamento debe crear cuentas exclusivas en los ordenadores de los empleados que solo tengan los permisos necesarios.
Instalar frezzeadores para que si instalan alguna aplicación al reiniciar la PC no se vea afectado.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos preventivos en los equipos que utilizan la digitalización de documentos.
Realizar actualizaciones del sistema previo análisis y verificación en el servidor de pruebas.
Deshabilitar los servicios del ordenador que no sean necesarios.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
</table>

Nombre del activo:	Digitalizador de documentos		
Área de preocupación: Interrupción en el servicio de energía eléctrica.			
Puntaje de riesgo relativo:23	**Probabilidad subjetiva:** Alto	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Adquirir un UPS exclusivo para el servidor en donde se almacenan los documentos y así evitar daños y pérdidas de información. • Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.			
Área de preocupación: Desastres Naturales			
Puntaje de riesgo relativo:33	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Realizar respaldo de información de los datos de la plataforma de recaudo y almacenarlos en la nube. • Crear un plan estratégico en caso de desastres naturales. • Mejorar la señalización en las oficinas. • Tener equipos en contra de incendios ubicados en lugares estratégicos.			

Tabla 279 Mitigación de riesgo del activo Digitalizador de Documentos
Fuente: Elaboración propia

Mitigación de riesgo del activo Documentos

Nombre del activo:	Documentos		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 24	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Solo personal autorizado puede generar documentos (facturas, solicitudes, actas, informes) • Los usuarios pueden generar el documento dependiendo del departamento que pertenece y el sistema que está utilizando a cuál debió acceder con el usuario y contraseña que le fue otorgada por el jefe de departamento tecnológico.			
Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.			
Puntaje de riesgo relativo: 15	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 4	**Acción:** Aceptar

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Documentos</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los documentos físicos deben estar resguardados en anaqueles o lugares fuera del alcance de personas ajenas a la oficina que pertenecen los documentos.
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna.
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo:28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Documentos</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo:15</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Instruir a los usuarios de un uso correcto de los dispositivos.
Programar mantenimientos continuos a los equipos (impresoras, PC, Laptop).
Tener en bodega repuestos que tienen más probabilidad de daño (fuente, procesador. Memoria RAM, disco duro, cables, titas)</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo:24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el personal de departamento tecnológico puede instalar y actualizar software.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.
Se debe comunicar a los empleados que no pueden instalar ningún software.
El departamento debe crear cuentas exclusivas en los ordenadores de los empleados que solo tengan los permisos necesarios.
Instalar frezzeadores para que si instalan alguna aplicación al reiniciar la PC no se vea afectado.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos preventivos en los equipos generan documentos.
Realizar actualizaciones del sistema previo análisis en el servidor de pruebas.
Deshabilitar los servicios del ordenador que no sean necesarios.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.</td></tr>
</table>

Nombre del activo:	Documentos		
Área de preocupación: Desastres Naturales			
Puntaje de riesgo relativo: 33	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Crear un plan estratégico en caso de desastres naturales. • Realizar respaldo de los documentos digitales y almacenarlos en la nube. • Mejorar la señalización en las oficinas. • Tener equipos en contra de incendios ubicados en lugares estratégicos.			

Tabla 280 Mitigación de riesgo del activo Documentos

Mitigación de riesgo del activo Intranet

Nombre del activo:	Intranet		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 25	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control • Solo el jefe de departamento tecnológico y el encargado de redes debe tener acceso a la administración de la intranet. • Los empleados de áreas que no tienen que ver con el departamento tecnológico deben tener acceso únicamente para realizar consultas en la intranet por medio del usuario y contraseña asignado por el jefe de departamento tecnológico • El jefe de departamento tecnológico debe realizar el cambio de contraseñas mensualmente. • Realizar copias de seguridad de las configuraciones de los dispositivos que tengan esta función. • Documentar los cambios que se realice en la intranet.			
Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.			
Puntaje de riesgo relativo: 15	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control • Realizar un instructivo para el uso adecuado de la intranet.			

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Intranet</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center, pero solo el jefe del departamento puede realizar modificaciones donde se encuentra la base de datos.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Instruir a los empleados para que utilicen correctamente los equipos.
Programar mantenimientos continuos de los dispositivos de red.
Tener en bodega repuestos que tienen más probabilidad de daño (switch, router, cables, tarjeta de red)</td></tr>
</table>

Nombre del activo:	Intranet		
Área de preocupación: Actualización o instalación de software sin autorización			
Puntaje de riesgo relativo: 19	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Solo el personal de departamento tecnológico puede instalar y actualizar software. • Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior. • Se debe comunicar a los empleados que no pueden instalar ningún software. • El departamento debe crear cuentas exclusivas en los ordenadores de los empleados que solo tengan los permisos necesarios. • Instalar frezzeadores para que si instalan alguna aplicación al reiniciar la PC no se vea afectado.			
Área de preocupación: Fallo o defecto de Software			
Puntaje de riesgo relativo: 19	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control: • Programar mantenimientos preventivos en los equipos que utilizan la intranet. • Realizar actualizaciones del sistema previo análisis en el servidor de pruebas. • Deshabilitar los servicios del ordenador que no sean necesarios. • Planificar revisión de las configuraciones de la intranet			
Área de preocupación: Interrupción en el servicio de energía eléctrica.			
Puntaje de riesgo relativo: 23	**Probabilidad subjetiva:** Alto	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Adquirir un UPS exclusivo los dispositivos de red y así evitar daños. • Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.			

Nombre del activo:	Intranet		
Área de preocupación: Desastres Naturales			
Puntaje de riesgo relativo: 24	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Crear un plan estratégico en caso de desastres naturales. • Mejorar la señalización en las oficinas. • Tener equipos en contra de incendios ubicados en lugares estratégicos.			

Tabla 281 Mitigación de riesgo del activo Intranet
Fuente: Elaboración propia

Mitigación de riesgo del activo Directorio Activo

Nombre del activo:	Directorio Activo		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 19	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control: • Solo el jefe de departamento tecnológico debe tener acceso a la administración del directorio activo. • Solo se puede ingresar al directorio activo con un usuario y contraseña. • El jefe de departamento tecnológico debe realizar cambiar su contraseña mensualmente, las contraseñas deben ser al menos 18 caracteres (letras mayúsculas y minúsculas, números, símbolos).			
Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.			
Puntaje de riesgo relativo: 19	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control: • Realizar un manual de uso del directorio activo.			

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Directorio Activo</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center, pero solo el jefe del departamento puede realizar modificaciones donde se encuentra instalado el directorio activo.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos al servidor de aplicaciones.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente. Memoria RAM, disco duro, cables)</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Directorio Activo</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico puede instalar y actualizar un componente de la base de datos.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar configuración de Servidores.
Realizar actualizaciones del sistema previo análisis en el servidor de pruebas.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.
Desinstalar los programas que no sean necesarios para la correcta funcionalidad del directorio activo.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo:33</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Adquirir un UPS exclusivo para el servidor de aplicaciones y así evitar daños, ya que en este se aloja el directorio activo.
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.</td></tr>
<tr><td colspan="4">Área de preocupación: Desastres Naturales</td></tr>
<tr><td>Puntaje de riesgo relativo:24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar respaldo de información de los datos del directorio activo y almacenarlos en la nube.
Crear un plan estratégico en caso de desastres naturales.
Mejorar la señalización en las oficinas que se realizan los cobros.
Tener equipos en contra de incendios ubicados en lugares estratégicos</td></tr>
</table>

Tabla 282 Mitigación de riesgo del activo Directorio Activo
Fuente: Elaboración propia

Mitigación de riesgo del activo Servidor de Aplicaciones

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo:33</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción:
Mitigar</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico debe tener acceso a la administración del servidor de aplicaciones.
Solo se puede ingresar con un usuario y contraseña.
El jefe de departamento tecnológico debe realizar el cambio de contraseña mensualmente, las contraseñas deben ser al menos 18 caracteres (letras mayúsculas y minúsculas, números, símbolos).
Colocar contraseña de la BIOS del servidor.
Realizar diariamente copias de seguridad.</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Se debe realizar un manual con las aplicaciones y configuraciones realizadas en el servidor.</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center. al data center se debe ingresar con la clave u implementar otra seguridad.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo:33</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción: Mitigar</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.
Implementar restricciones en firewall.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos servidores.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente. Memoria RAM, disco duro, cables)
Adecuar zona para el enfriamiento de los servidores.
Verificar el voltaje de la toma corriente</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo:19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría:
Grupo 3</td><td>Acción:
Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico puede instalar y actualizar un componente de la base de datos.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de Aplicaciones</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo: 36</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción: Mitigar</td></tr>
<tr><td colspan="4">Control:
Verificar las licencias de los sistemas instalados.
Planificar configuración de Servidores.
Realizar pruebas de carga al sistema.
Instalar antivirus en cada uno de los servidores de la entidad
Deshabilitar o desinstalar servicios que no sean necesarios.
Antes de instalar actualizaciones de nuevas versiones se debe realizar evaluaciones en el servido de pruebas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo: 33</td><td>Probabilidad subjetiva: Alto</td><td>Categoría:
Grupo 1</td><td>Acción:
Mitigar</td></tr>
<tr><td colspan="4">Control:
Adquirir un UPS exclusivo para el servidor de aplicaciones y así evitar daños.
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad</td></tr>
<tr><td colspan="4">Área de preocupación: Desastres Naturales</td></tr>
<tr><td>Puntaje de riesgo relativo: 40</td><td>Probabilidad subjetiva: Medio</td><td>Categoría:
Grupo 2</td><td>Acción:
Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Realizar respaldo del servidor de aplicaciones y almacenarlos en la nube o dispositivo de almacenamiento ubicado en otra zona geográfica.
Crear un plan estratégico en caso de desastres naturales.
Mejorar la señalización en las oficinas.
Tener equipos en contra de incendios ubicados en lugares estratégicos.</td></tr>
</table>

Tabla 283 Mitigación de riesgo del activo Servidor de Aplicaciones
Fuente: Elaboración propia

Mitigación de riesgo del activo Servidor de Desarrollo

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de Desarrollo</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo:28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico y encargado de desarrollo deben tener acceso a la administración del servidor de aplicaciones.
Solo se puede ingresar con un usuario y contraseña.
El jefe de departamento tecnológico debe realizar el cambio de contraseña mensualmente, las contraseñas deben ser al menos 18 caracteres (letras mayúsculas y minúsculas, números, símbolos).
Colocar contraseña de la BIOS del servidor.
Realizar diariamente copias de seguridad.</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Se debe realizar un manual con las aplicaciones y configuraciones realizadas en el servidor.</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo: 28</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center. al data center se debe ingresar con la clave u implementar otra seguridad.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de Desarrollo</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 24</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.
Implementar restricciones en firewall.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo:24</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos servidores.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente. Memoria RAM, disco duro, cables)
Adecuar zona para el enfriamiento de los servidores.
Verificar el voltaje de la toma corriente</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo:15</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 4</td><td>Acción: Aceptar</td></tr>
<tr><td colspan="4">Control:
Solo el jefe de departamento tecnológico y encargado de desarrollo pueden instalar y actualizar un componente de la base de datos.
Se debe realizar copias de seguridad del sistema para poderlos restaurar a una versión anterior.</td></tr>
</table>

Nombre del activo:	Servidor de Desarrollo		
Área de preocupación: Fallo o defecto de Software			
Puntaje de riesgo relativo:23	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 3	**Acción:** Transferir o Aceptar
Control: • Verificar las licencias de los sistemas instalados. • Planificar configuración de Servidores. • Realizar pruebas de carga al sistema. • Instalar antivirus en cada uno de los servidores de la entidad • Deshabilitar o desinstalar servicios que no sean necesarios. • Antes de instalar actualizaciones de nuevas versiones se debe realizar evaluaciones en el servido de pruebas.			
Área de preocupación: Interrupción en el servicio de energía eléctrica.			
Puntaje de riesgo relativo: 33	**Probabilidad subjetiva:** Alto	**Categoría:** Grupo 1	**Acción:** Mitigar
Control: • Adquirir un UPS exclusivo para el servidor de desarrollo y así evitar daños. • Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad.			
Área de preocupación: Desastres Naturales			
Puntaje de riesgo relativo: 37	**Probabilidad subjetiva:** Medio	**Categoría:** Grupo 2	**Acción:** Mitigar o Transferir
Control: • Crear un plan estratégico en caso de desastres naturales. • Mejorar la señalización en las oficinas. • Tener equipos en contra de incendios ubicados en lugares estratégicos.			

Tabla 284 Mitigación de riesgo del activo Servidor de Desarrollo
Fuente: Elaboración propia

Mitigación de riesgo del activo Servidor de Pruebas

Nombre del activo:	Servidor de pruebas		
Área de preocupación: Exposición de los activos de información, acceso no autorizado a los sistemas informáticos.			
Puntaje de riesgo relativo: 15	**Probabilidad subjetiva:** Bajo	**Categoría:** Grupo 4	**Acción:** Aceptar
Control: • Solo los integrantes del departamento tecnológico pueden acceder al servidor de pruebas. • Realizar cambios de contraseña mensualmente. • Colocar contraseña de la BIOS del servidor.			

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de pruebas</td></tr>
<tr><td colspan="4">Área de preocupación: Desconocimiento en el manejo de los sistemas informáticos.</td></tr>
<tr><td>Puntaje de riesgo relativo:19</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Se debe realizar un manual con las aplicaciones y configuraciones realizadas en el servidor.
Se deben realizar informes de los resultados de las pruebas obtenidas de aplicaciones, actualizaciones, configuraciones, etc.</td></tr>
<tr><td colspan="4">Área de preocupación: Exposición de los activos de información, acceso no autorizado a la infraestructura física.</td></tr>
<tr><td>Puntaje de riesgo relativo:19</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Los integrantes del departamento tecnológico son los únicos que pueden ingresar a la data center.
Crear un registro para el ingreso al data center.
Añadir mayor seguridad al ingreso al data center (candados, sistema por medio de claves).
Añadir cámaras de vigilancia en la tanto en la oficina del departamento tecnológico como en data center. al data center se debe ingresar con la clave u implementar otra seguridad.</td></tr>
<tr><td colspan="4">Área de preocupación: Problemas de conectividad en la red interna de la organización.</td></tr>
<tr><td>Puntaje de riesgo relativo: 15</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 3</td><td>Acción: Transferir o Aceptar</td></tr>
<tr><td colspan="4">Control:
Planificar revisiones de los dispositivos de la red interna
Configurar restricciones de firewall en el servidor.
El ingeniero encargado de redes y jefe de departamento tecnológico son los únicos que pueden realizar modificaciones a la red interna de la organización.
Crear un registro de las modificaciones realizadas.
Implementar restricciones en firewall.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de internet</td></tr>
<tr><td>Puntaje de riesgo relativo: 19</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
La entidad deberá contar con un proveedor alterno en caso que el proveedor de internet principal presente fallas.</td></tr>
</table>

<table>
<tr><td>Nombre del activo:</td><td colspan="3">Servidor de pruebas</td></tr>
<tr><td colspan="4">Área de preocupación: Falla en los componentes de hardware de los equipos</td></tr>
<tr><td>Puntaje de riesgo relativo: 15</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 4</td><td>Acción: Aceptar</td></tr>
<tr><td colspan="4">Control:
Programar mantenimientos continuos servidores.
Tener en bodega repuestos que tienen más probabilidad de daño (fuente. Memoria RAM, disco duro, cables)
Adecuar zona para el enfriamiento de los servidores.
Verificar el voltaje de la toma corriente</td></tr>
<tr><td colspan="4">Área de preocupación: Actualización o instalación de software sin autorización</td></tr>
<tr><td>Puntaje de riesgo relativo:15</td><td>Probabilidad subjetiva: Bajo</td><td>Categoría: Grupo 4</td><td>Acción: Aceptar</td></tr>
<tr><td colspan="4">Área de preocupación: Fallo o defecto de Software</td></tr>
<tr><td>Puntaje de riesgo relativo:19</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Verificar las licencias de los sistemas instalados.
Planificar configuración de Servidores.
Realizar pruebas de carga al sistema.
Instalar antivirus en cada uno de los servidores de la entidad
Deshabilitar o desinstalar servicios que no sean necesarios.
Antes de instalar actualizaciones de nuevas versiones se debe realizar evaluaciones en el servido de pruebas.</td></tr>
<tr><td colspan="4">Área de preocupación: Interrupción en el servicio de energía eléctrica.</td></tr>
<tr><td>Puntaje de riesgo relativo:17</td><td>Probabilidad subjetiva: Alto</td><td>Categoría: Grupo 2</td><td>Acción: Mitigar o Transferir</td></tr>
<tr><td colspan="4">Control:
Adquirir un UPS exclusivo para el servidor de pruebas y así evitar daños.
Adquirir un generador de energía que abastezca a toda la institución y restablecer las actividades a su normalidad</td></tr>
<tr><td colspan="4">Área de preocupación: Desastres Naturales</td></tr>
<tr><td>Puntaje de riesgo relativo: 15</td><td>Probabilidad subjetiva: Medio</td><td>Categoría: Grupo 4</td><td>Acción: Aceptar</td></tr>
<tr><td colspan="4">Control:
Crear un plan estratégico en caso de desastres naturales.
Mejorar la señalización en las oficinas.
Tener equipos en contra de incendios ubicados en lugares estratégicos.</td></tr>
</table>

Tabla 285 Mitigación de riesgo del activo Servidor de Pruebas
Fuente: Elaboración propia

ANEXO J: Fotografías

Fig. 23 Oficina del Departamento Tecnológico (Ing. Luis Carrasco, jefe del Departamento)
Fuente: Elaboración propia

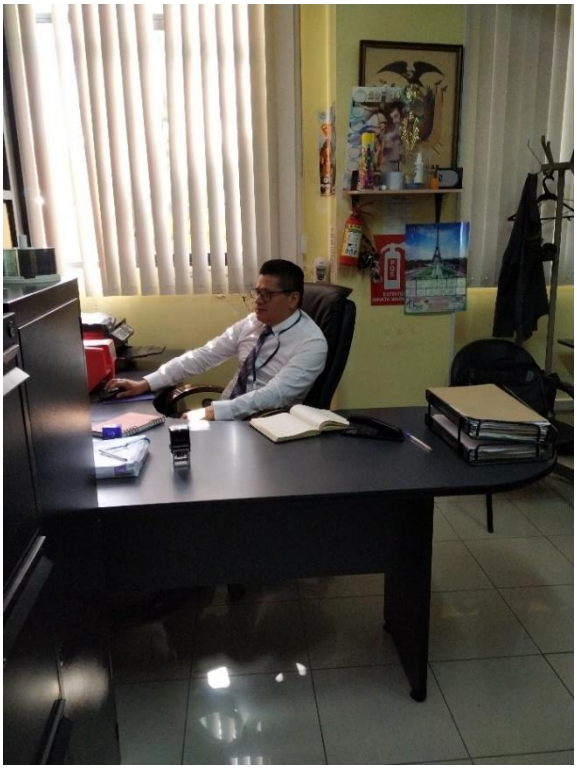


Fig. 24 Oficina del Departamento Tecnológico (Ing. Julio Flores, Encargado de redes)
Fuente: Elaboración propia

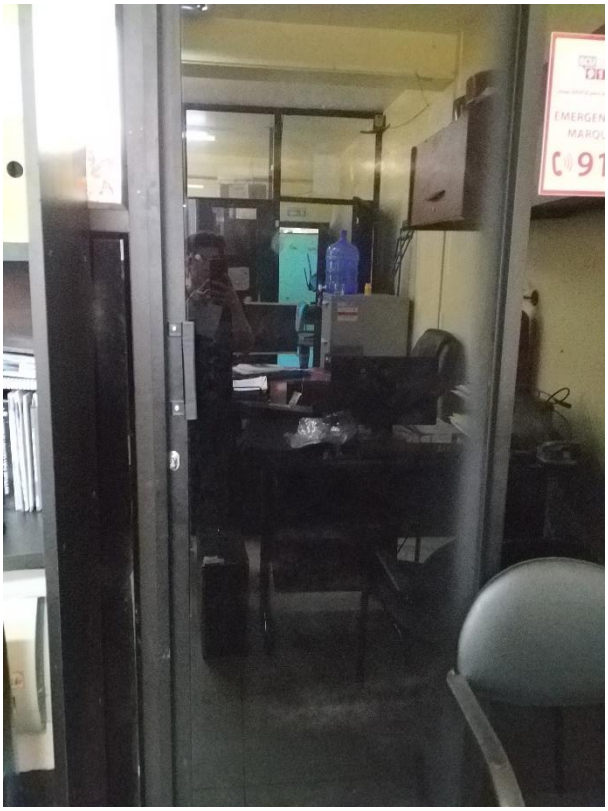


Fig. 25 Ingreso al data center

Fuente: Propia

Fig. 26Dispositivo de enfriamiento portátil

Fuente: Propia

Fig. 27 Servidores de Aplicaciones, Desarrollo y Pruebas

Fuente: Propia

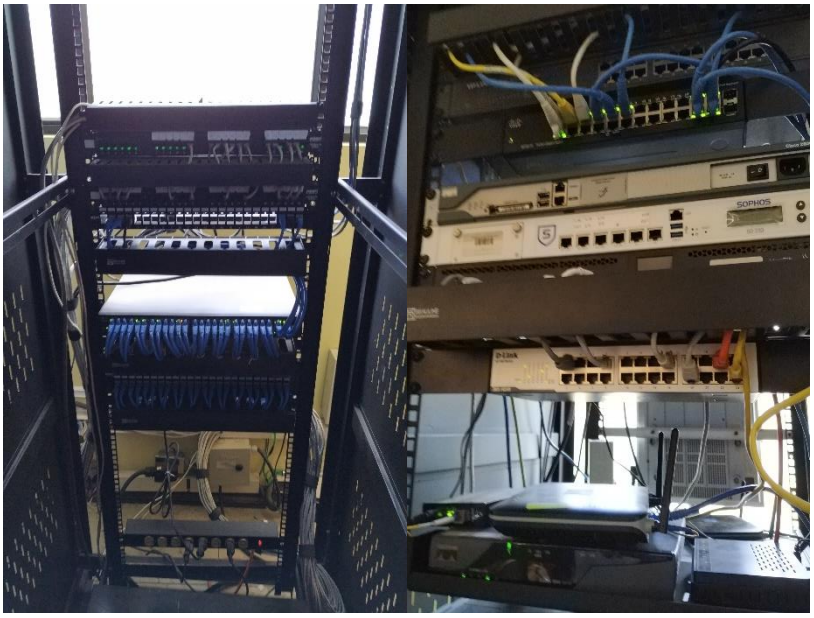


Fig. 28Dispositivos de Red interna

Fuente: Propia

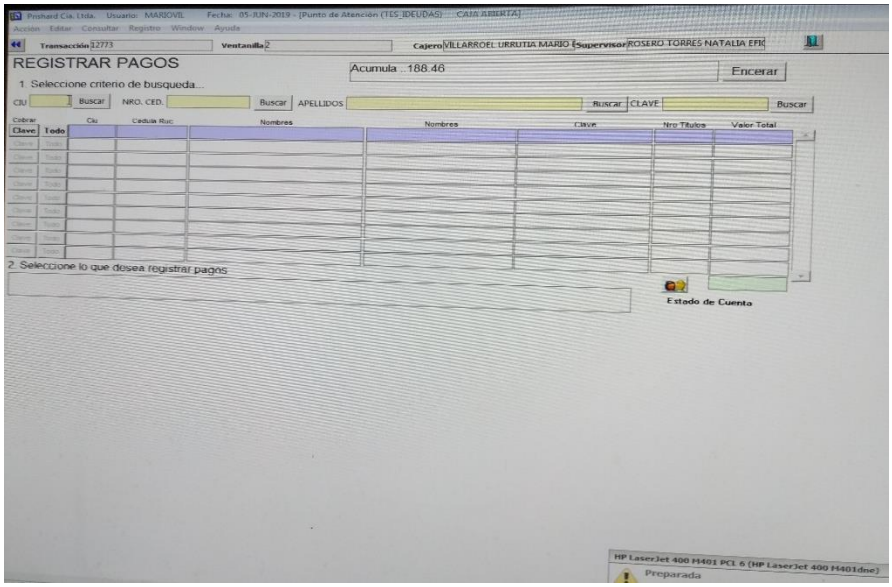


Fig. 29 Plataforma de Recaudo

Fuente: Propia

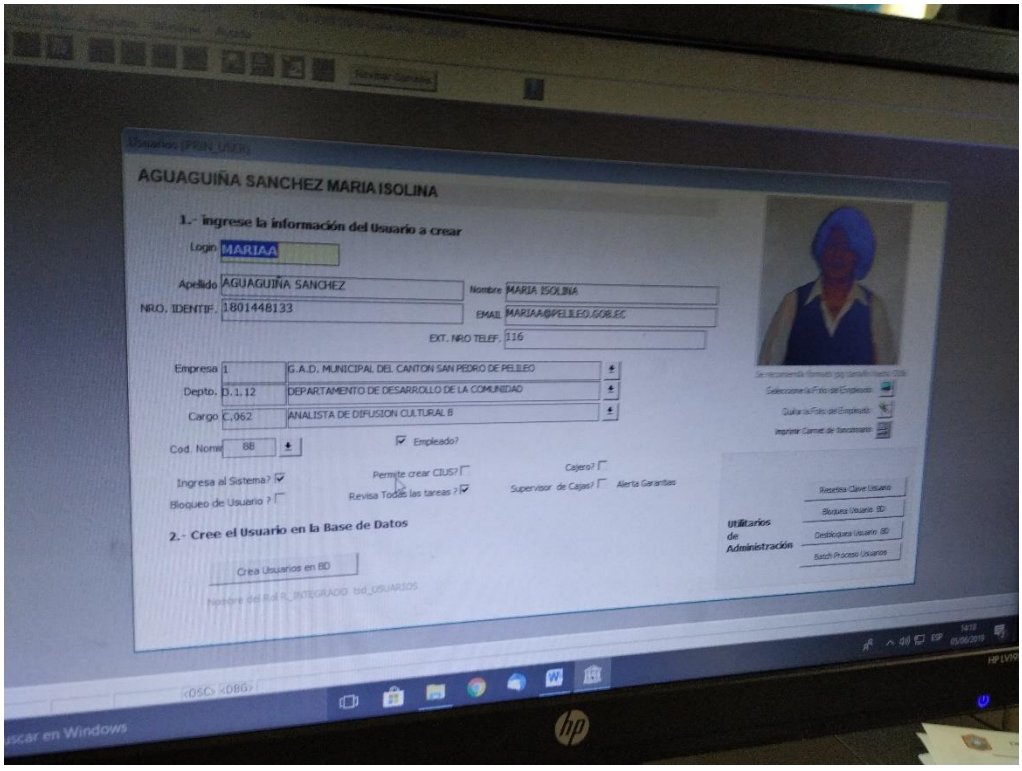


Fig. 30 Directorio Activo

Fuente: Propia

Fig. 31 Pagina de la intranet (Soporte, SMS Online, Correo)

Fuente: Propia

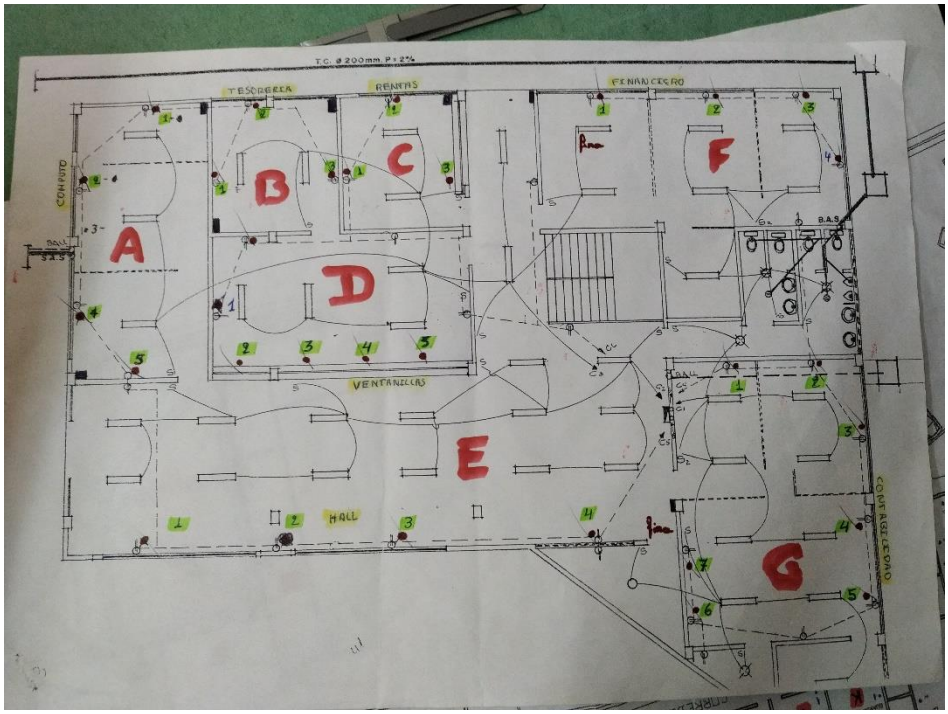
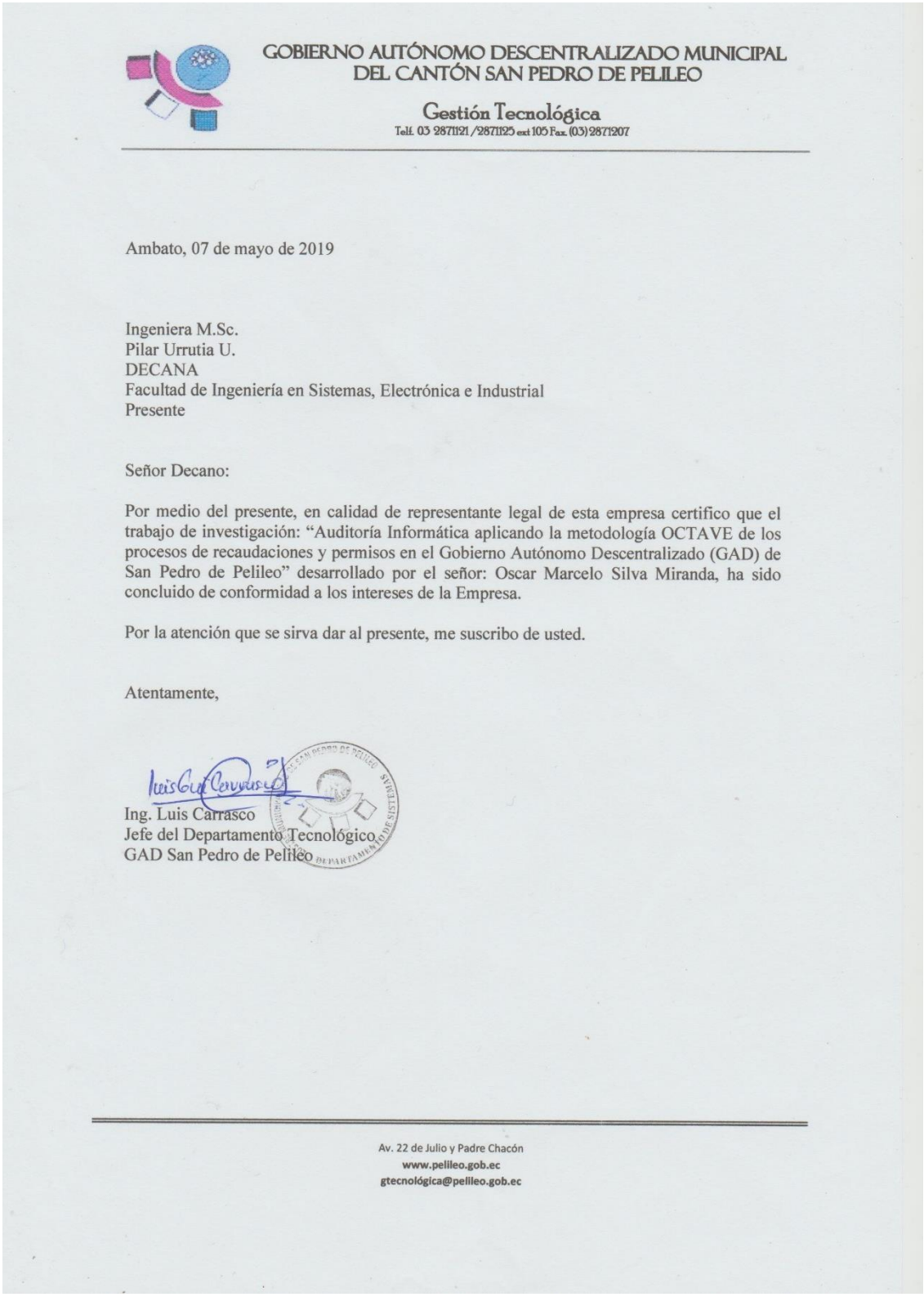


Fig. 32 Distribución de Red Interna

Fuente: Propia

ANEXO K: Finalización



GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL
DEL CANTÓN SAN PEDRO DE PELILEO

Gestión Tecnológica
Telf. 03 2871121 /2871125 ext 105 Fax. (03) 2871207

Ambato, 07 de mayo de 2019

Ingeniera M.Sc.
Pilar Urrutia U.
DECANA
Facultad de Ingeniería en Sistemas, Electrónica e Industrial
Presente

Señor Decano:

Por medio del presente, en calidad de representante legal de esta empresa certifico que el trabajo de investigación: "Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo" desarrollado por el señor: Oscar Marcelo Silva Miranda, ha sido concluido de conformidad a los intereses de la Empresa.

Por la atención que se sirva dar al presente, me suscribo de usted.

Atentamente,

Ing. Luis Carrasco
Jefe del Departamento Tecnológico
GAD San Pedro de Pelileo

Av. 22 de Julio y Padre Chacón
www.pelileo.gob.ec
gtecnológica@pelileo.gob.ec

Fig. 33 Finalización de Proyecto